Core Program Week 1

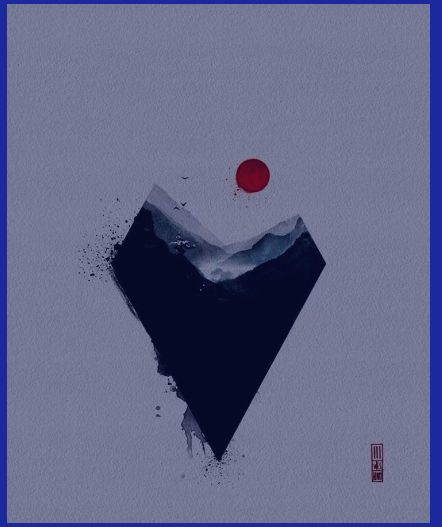
zkSNARKの基礎

ZK Tokyo

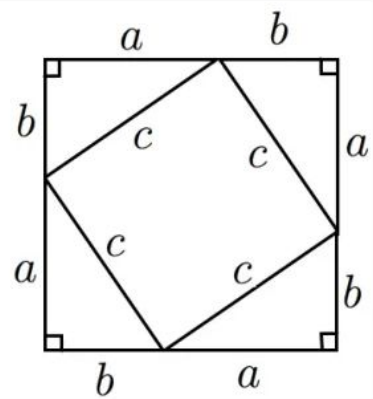
目次

- ゼロ知識証明
- zkSNARK
- SNARKの商用化
- セットアップ
- 効率的なSNARKの構築

ゼロ知識証明



証明



図において大きい正方形の面積 S を二通りで表す。

- 一辺$(a+b)$ の正方形なので $S=(a+b)^2$
- 一辺 c の正方形と直角三角形4つの和なので，$S=c^2+4\cdot\frac{1}{2}ab$

よって，$(a+b)^2=c^2+2ab$

整理すると $a^2+b^2=c^2$

となり三平方の定理を得る。

前提: 正方形と三角形の面積公式

主張: $a^2 + b^2 = c^2$

仮定: 直角三角形4つを正方形の中に収める

証明
(=論理的推論)

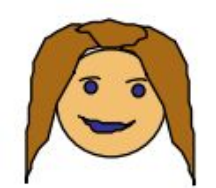
証明のプロトコル

主張

前提

仮定

証明者



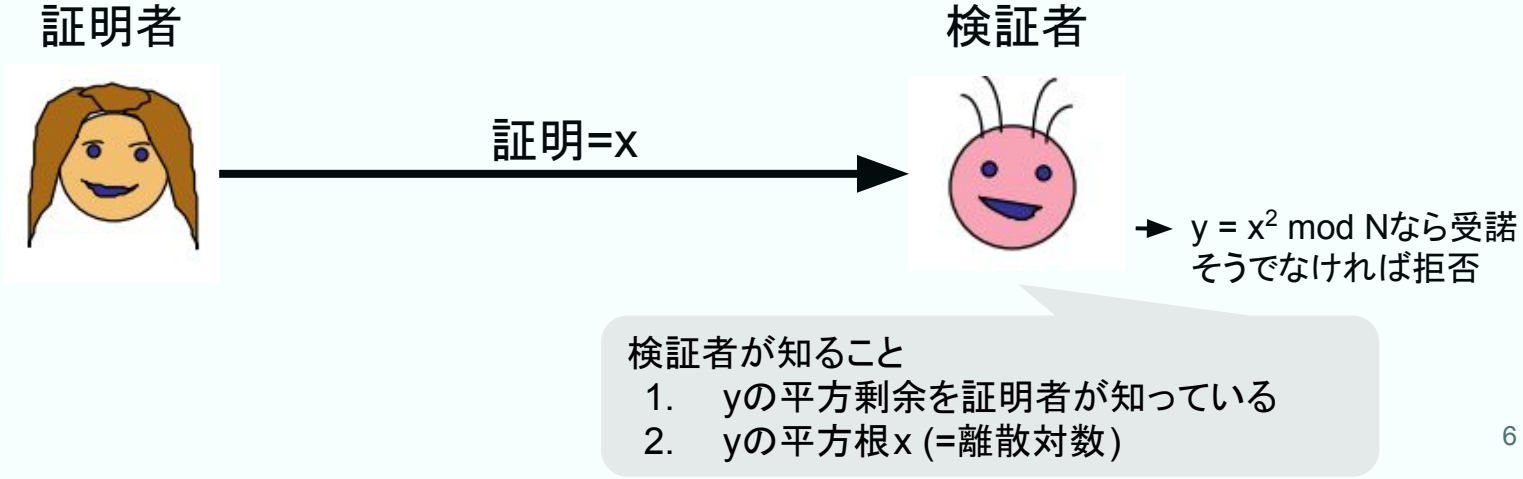
証明

検証者

→ 受諾/拒否

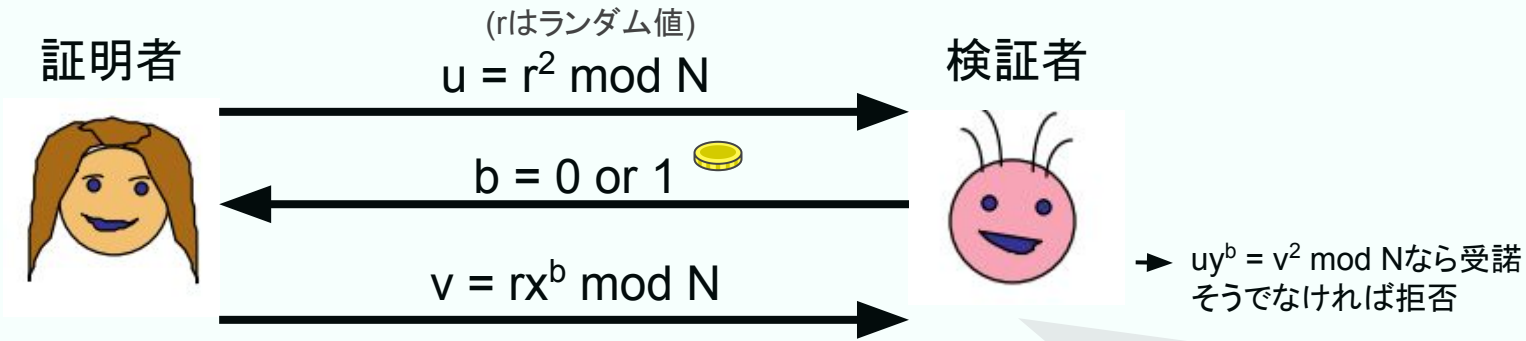
例: 平方剰余数の証明

主張: mod Nにおけるyの平方根xを知っている



平方剰余数のゼロ知識対話型証明

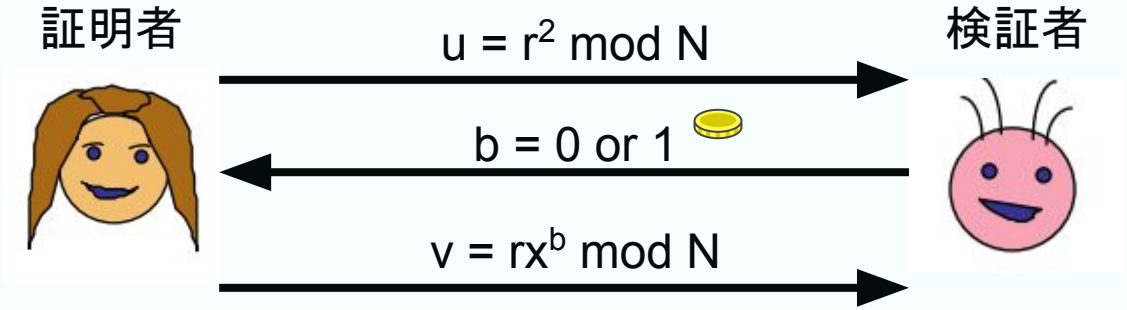
主張: mod Nにおけるyの平方根xを知っている



検証者が知ること
1. xがyの平方剰余であること

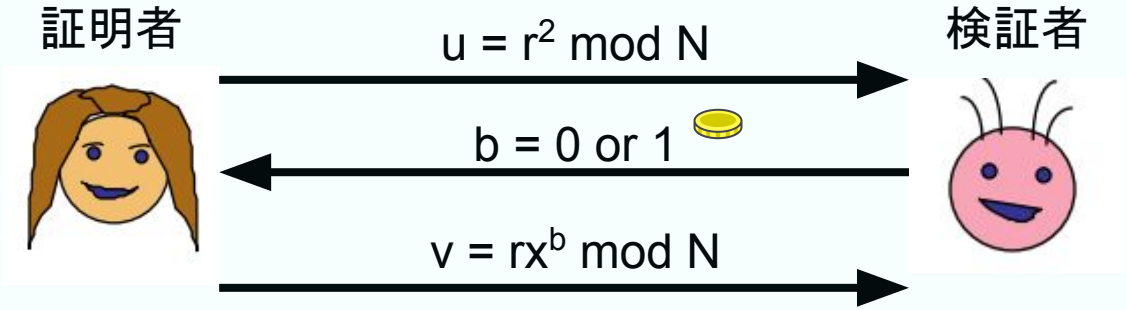
ゼロ知識証明とは

主張: mod Nにおけるyの平方根xを知っている



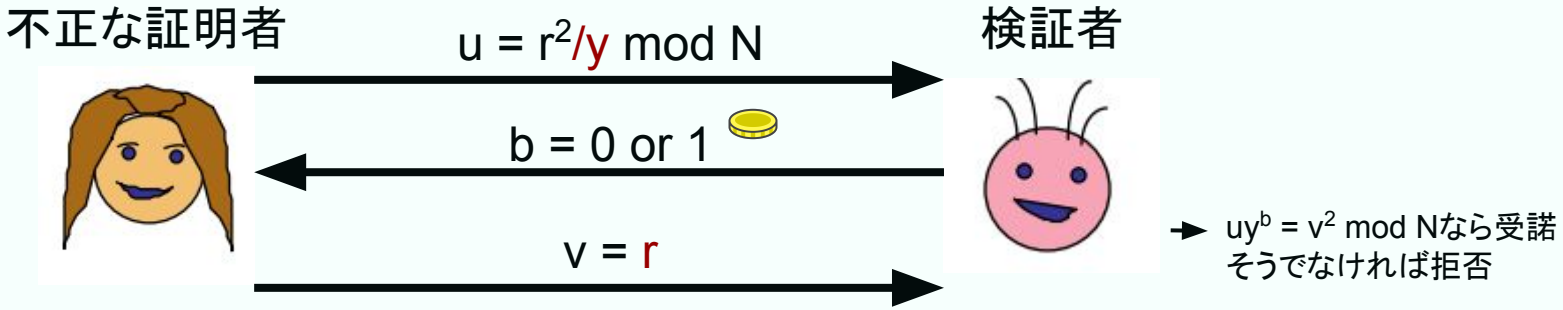
1. **完全性**: 主張が正しいならば検証者は受諾する
2. **健全性**: 主張が正しくないならば検証者は高確率で拒否する
3. **ゼロ知識**: 検証者はxについて何の情報も得られない

完全性: 主張が正しいならば検証者は受諾する



b=1ならr^2x^2 mod N
b=0ならr^2 mod N
で常に等式が成り立つ

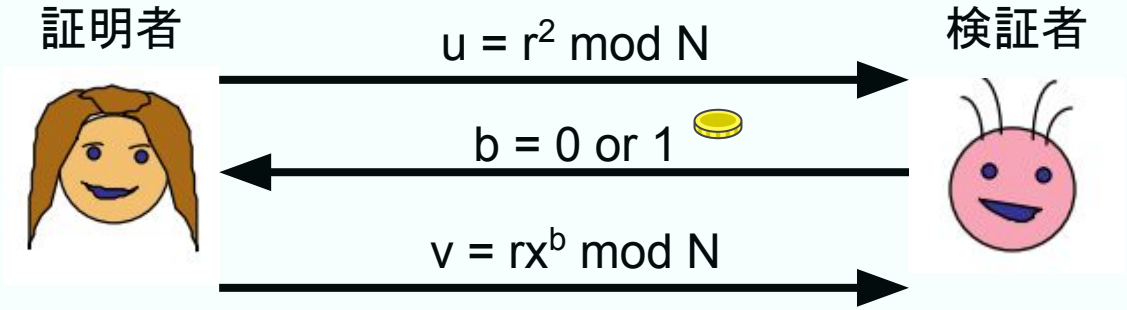
健全性: 主張が正しくないならば検証者は高確率で拒否する



b=1なら受諾
b=0なら拒否
受諾する確率は 1/2

100回繰り返せば受諾する確率は$(1/2)^{100}$

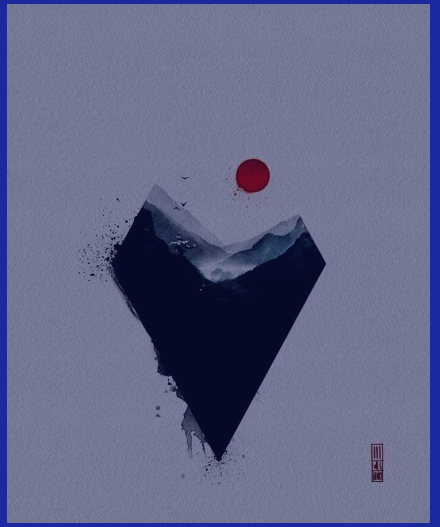
ゼロ知識：検証者はxについて何の情報も得られない



u, v, yからxを計算するのは困難
(離散対数)

ZK Tokyo

zkSNARK



SNARKとは

簡潔で　非対話な　知識の証明

SNARK (Succinct Non-interactive ARgument of Knowledge)

- 例:「私はSHA256(m)=0の原像mを知っている」
- 簡潔とは？
  - 証明が短い
  - 検証が速い
- zkSNARK
  - 証明はmについて何も開示しない

SNARKの歴史

対話型証明とゼロ知識証明という概念の誕生

The Knowledge Complexity of Interactive Proof-Systems

(Extended Abstract)

Shafi Goldwasser MIT
Silvio Micali MIT
Charles Rackoff University of Toronto

NP問題はすべてゼロ知識対話型証明にできることが証明

Everything Provable is Provable in Zero-Knowledge

Michael Ben-Or — Hebrew University
Oded Goldreich — Technion – Israel Institute of Technology
Shafi Goldwasser — M.I.T. Laboratory for Computer Science
Johan Håstad — Royal Institute of Technology, Sweden
Joe Kilian — M.I.T. Laboratory for Computer Science
Silvio Micali — M.I.T. Laboratory for Computer Science
Phillip Rogaway — M.I.T. Laboratory for Computer Science

zkSNARKが実用的に

Pinocchio: Nearly Practical Verifiable Computation

Bryan Parno, Jon Howell — *Microsoft Research*
Craig Gentry, Mariana Raykova — *IBM Research*

1985年

Fiat-Shamir変換

How To Prove Yourself:
Practical Solutions to Identification
and Signature Problems

Amos Fiat and Adi Shamir
Department of Applied Mathematics
The Weizmann Institute of Science
Rehovot 76100, Israel

1992年

対話型証明は多項式空間で検証できることが証明

IP = PSPACE

ADI SHAMIR

The Weizmann Institute of Science, Rehovot, Israel

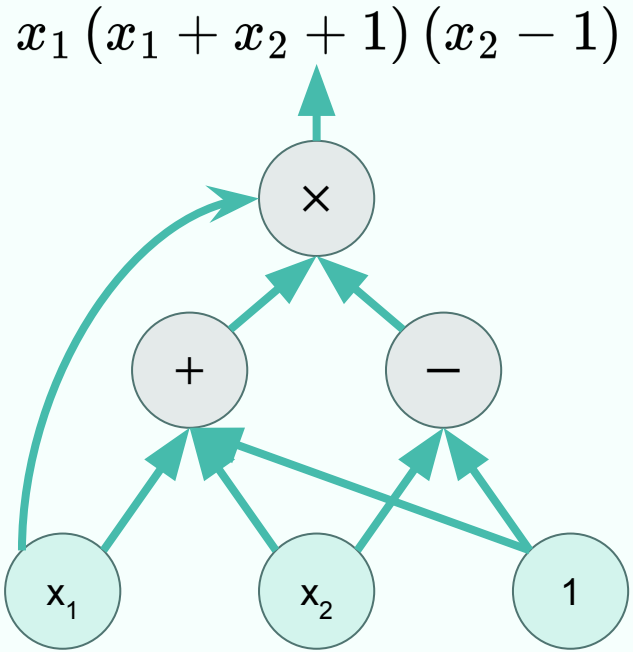
2013年

Groth16, Plonk, Marlin, Bulletproofs, STARKなどが登場

補足資料

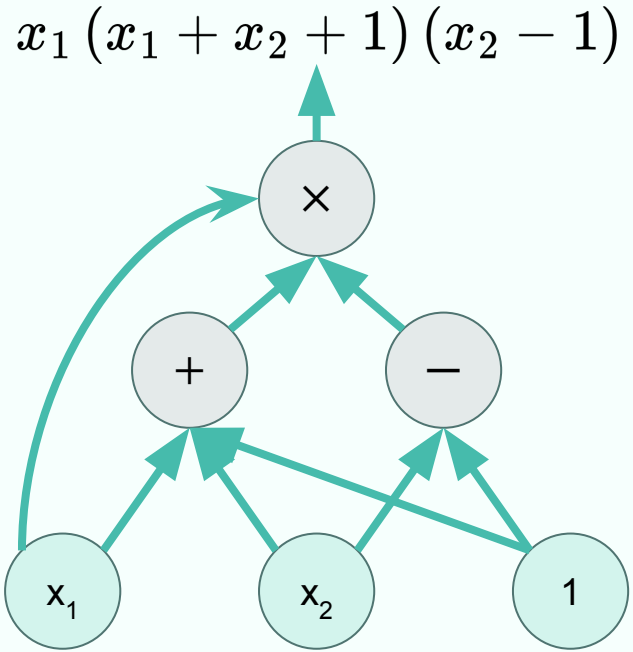
なぜ算術回路 (Arithmetic Circuit)？

- SNARKでは算術回路がよく用いられる
- 算術回路は多項式をグラフで表現したもの
- 任意の計算を表現できる汎用性✅
- 多項式に帰着するアルゴリズムとの相性✅
- 一方で多項式以外は扱えない (e.g. 2^n)
    - 次数上限を設けることで多項式表現したり、多項式近似でカバーできる



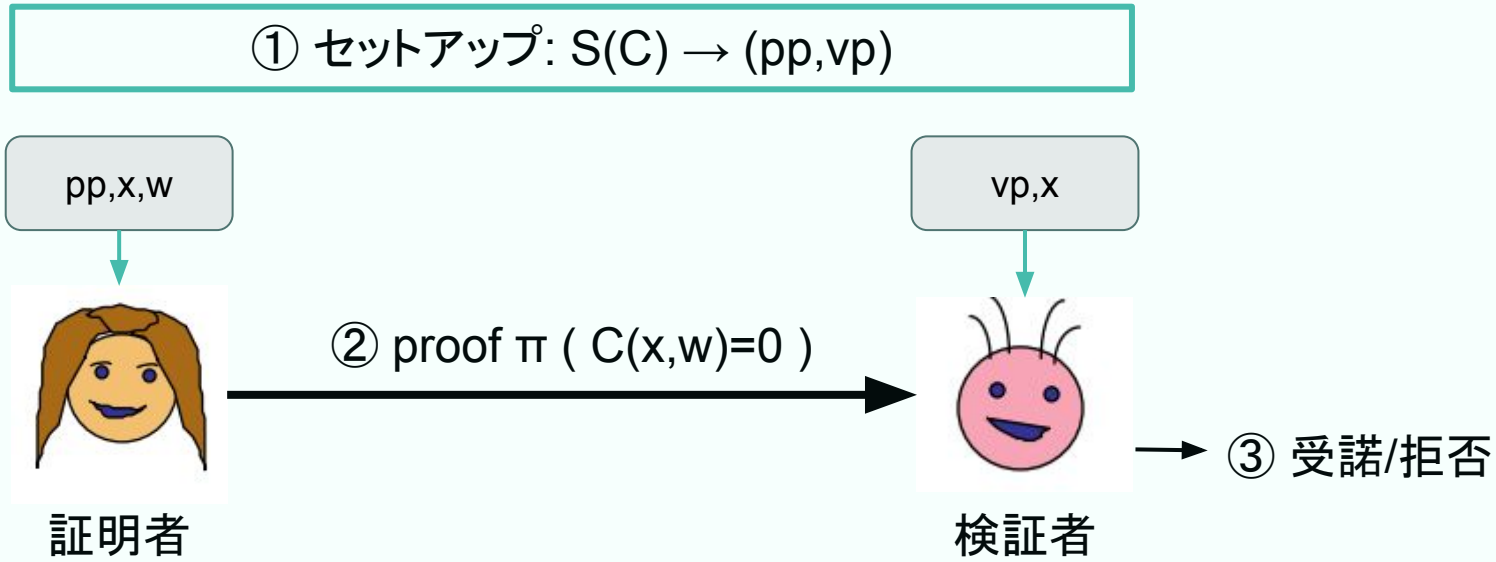
算術回路 (Arithmetic Circuit)

- n個の有限体F^nを入力としてFを出力する
  - C: $F^n \to F$
- n変数多項式を定義する
- $|C|$ = Cのゲート数



SNARKプロトコル

- 回路 C(x,w): $F^n \rightarrow F$ が与えられたとき
  - F^nのうち xは公開する値、wは秘密の値(witness)



SNARKの要件

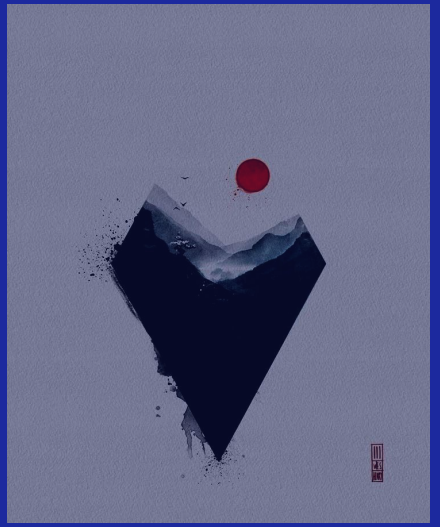
ZK
- **ゼロ知識: 検証者はwについて何の情報も得られない**

Succinct
- **簡潔: 証明サイズがpolylog(|C|)で検証時間がO(|x|, polylog(|C|))**

NARK
- **完全性**: C(x,w)=0を満たすwを知っているならば検証者は受諾する
- **健全性**: C(x,w)=0を満たすwを知らないならば検証者は高確率で拒否する

https://rdi.berkeley.edu/zk-learning/assets/Lecture2-2023.pdf (pp. 25)

セットアップ



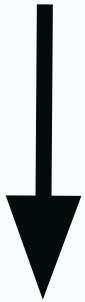
SNARK構築に立ちはだかる壁

- wは長すぎる...
- Cを直接実行するのは難しい...
- wは公開したくない...

Cの小さな要約vpを事前に計算して
効率的に検証可能な問題に置き換えよう！

セットアップ

- S(C;r) → (pp,vp)
  - rはランダムビット
  - ppはprover parameter
  - vpはverifier parameter



より安全

Trusted Setup: rは証明者に秘密でなければならない

Trusted but universal Setup: pp,vpは回路に対して独立

Transparent Setup: セットアップに秘密の値が必要ない

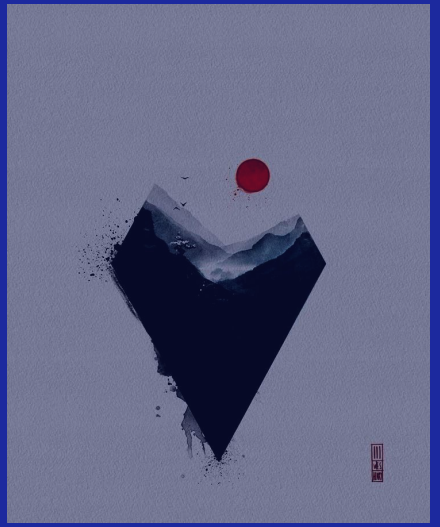
近年のzkSNARKsの進捗

$|C|=2^{20}$

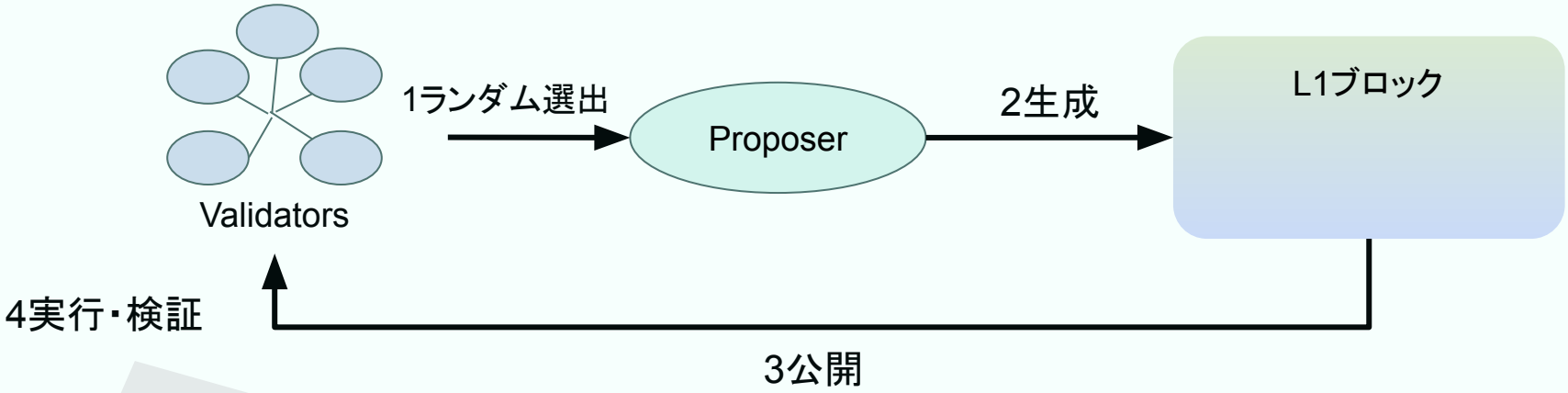
	証明サイズ	検証時間	セットアップ	量子耐性
Groth'16	200B (constant)	1.5ms (constant)	trusted	❌
Plonk / Marlin	400B (constant)	3ms (constant)	universal trusted	❌
Bulletproofs	1.5kB (log)	3s (linear)	transparent	❌
FRI-STARK	100kB ($\log^2$)	10ms ($\log^2$)	transparent	✅

参考: https://github.com/matter-labs/awesome-zero-knowledge-proofs

SNARKの商用化



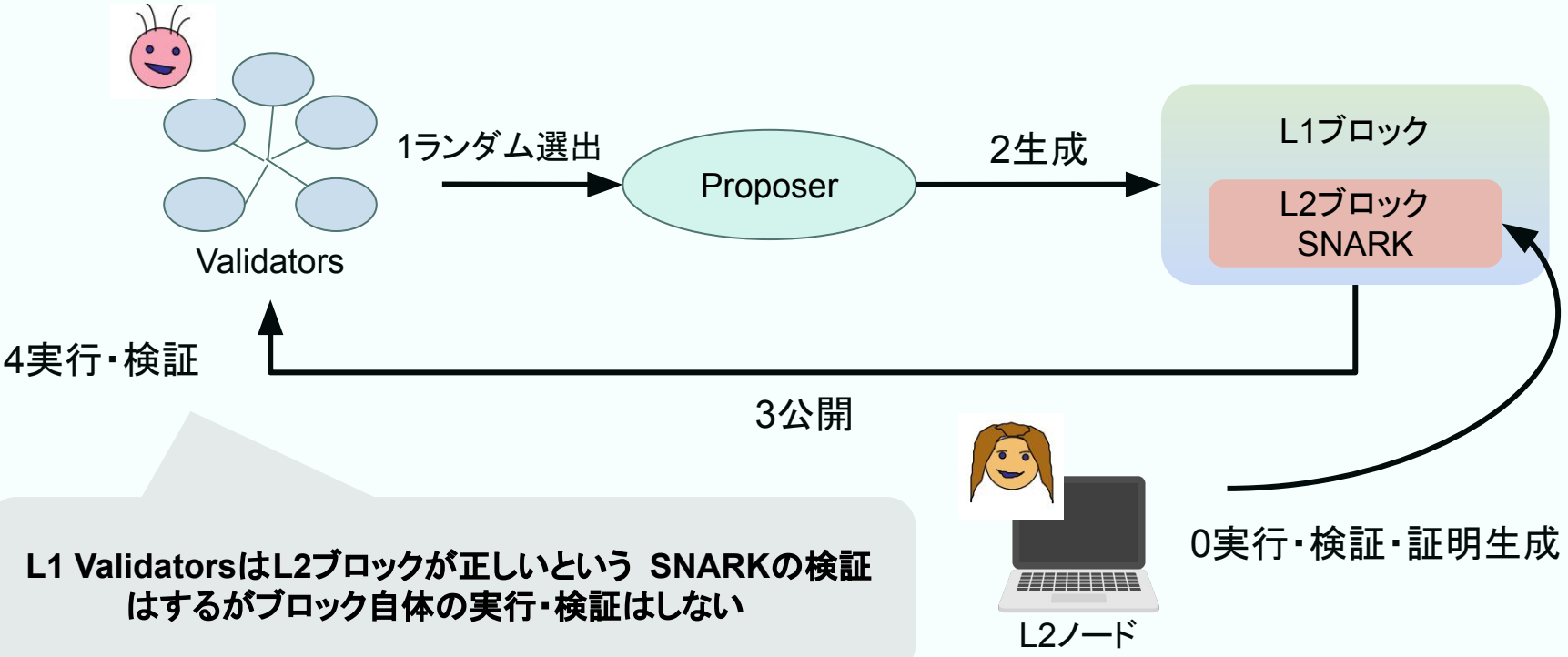
Ethereumのスケーラビリティ問題



スケールしない！
(バリデータ数・トランザクション・プログラムサイズとか色んな意味で)

https://www.docswell.com/s/linoscope/582D91-2025-04-05-174750#p12

zkRollup

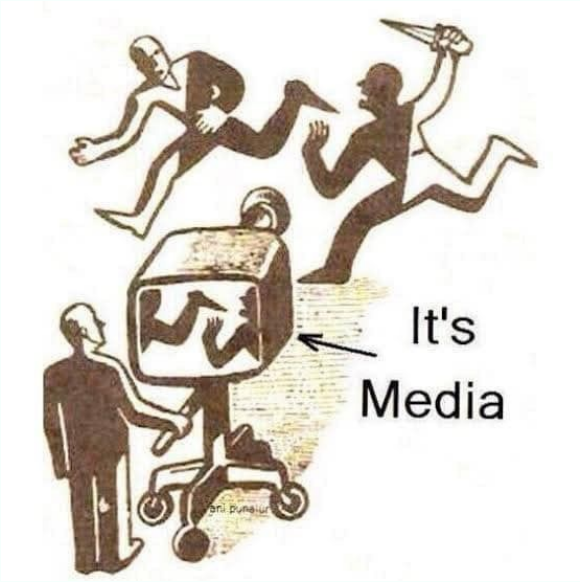


L1 ValidatorsはL2ブロックが正しいという SNARKの検証はするがブロック自体の実行・検証はしない

https://www.docswell.com/s/linoscope/582D91-2025-04-05-174750#p12

偽情報問題

- ディープフェイクやメディアによる悪質な印象操作は社会問題



https://www.nikkei.com/article/DGXZQOGN177EW0X10C22A3000000/

C2PA (Coalition for Content Provenance and Authenticity)

署名

zkSNARK

検証者

カメラが署名

この画像には
少女を切り取る加工がされており、恣意的な加工はされてない！

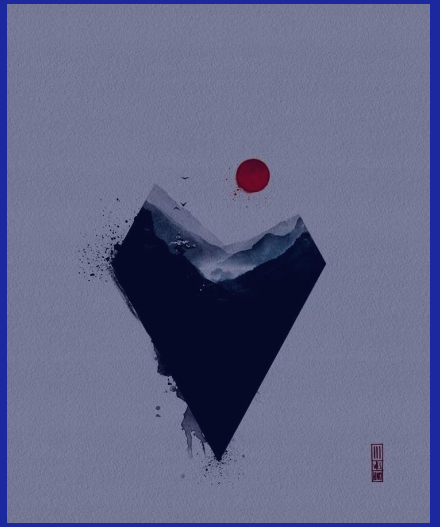
https://c2pa.org/

その他のサービス例

- **プライベート送金（Tornado Cash , Railgun)**
  送金先を隠した送金を行う
- **zkPoEX**
  DeFiに対してバグを起こさせる入力パターンを知っていることを入力を秘匿しつつ証明してバグ報奨金を受け取る
- **オンランプ/オフランプ（ZKP2P)**
  Fiatと暗号資産を安全に交換する

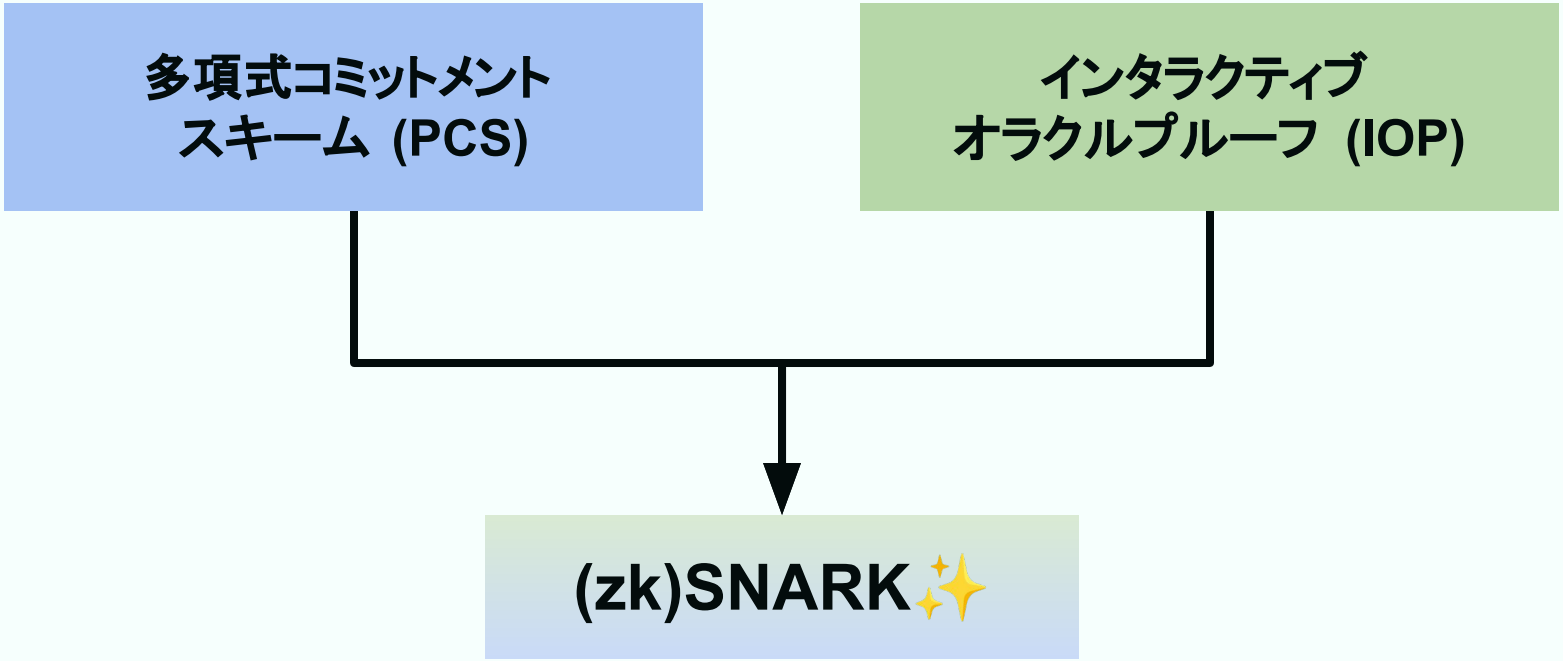
https://vitalik.eth.limo/general/2022/06/15/using_snarks.html

効率的なSNARKの構築



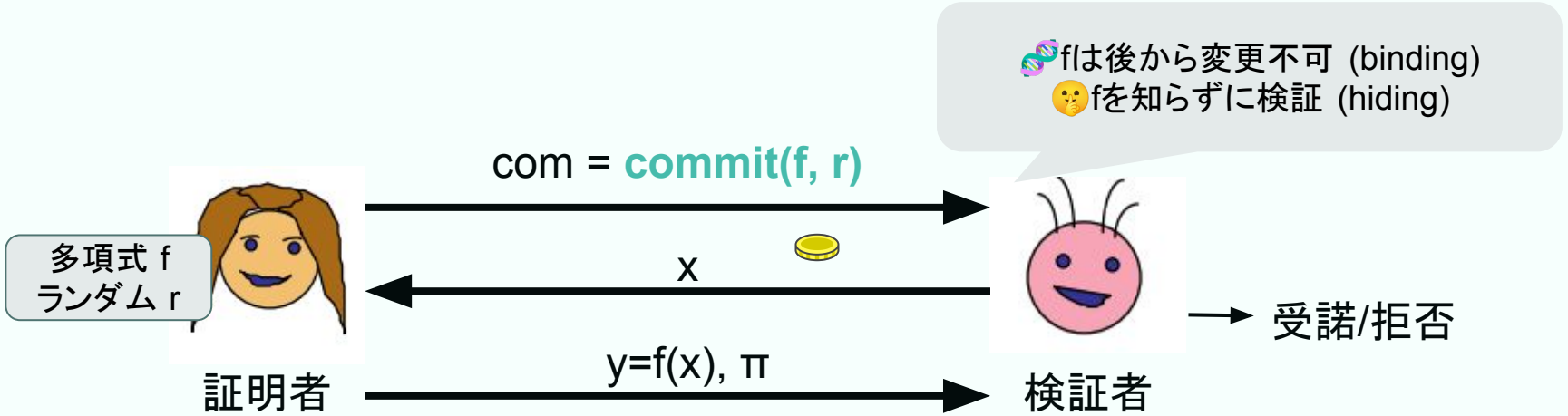
汎用的な回路に対する SNARKの構築

(IP, PCPなどもあり)



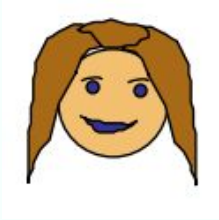
多項式コミットメントスキーム (PCS)

- 前提: 主張を多項式fの形式に変換
- 主張: f(x)=yを証明する
- **commit(f,r) → com**: 多項式の使用を事前に宣言し、
- **verify(com, x, y, π)**: 評価が正しいことを検証する



オラクルって？

- なにかを即答してくれる万能箱
- 天気オラクル：天気を即答してくれる
- ランダムオラクル：完全なランダム値を即答してくれる
- 多項式オラクル：多項式評価 f(z)を即答してくれる



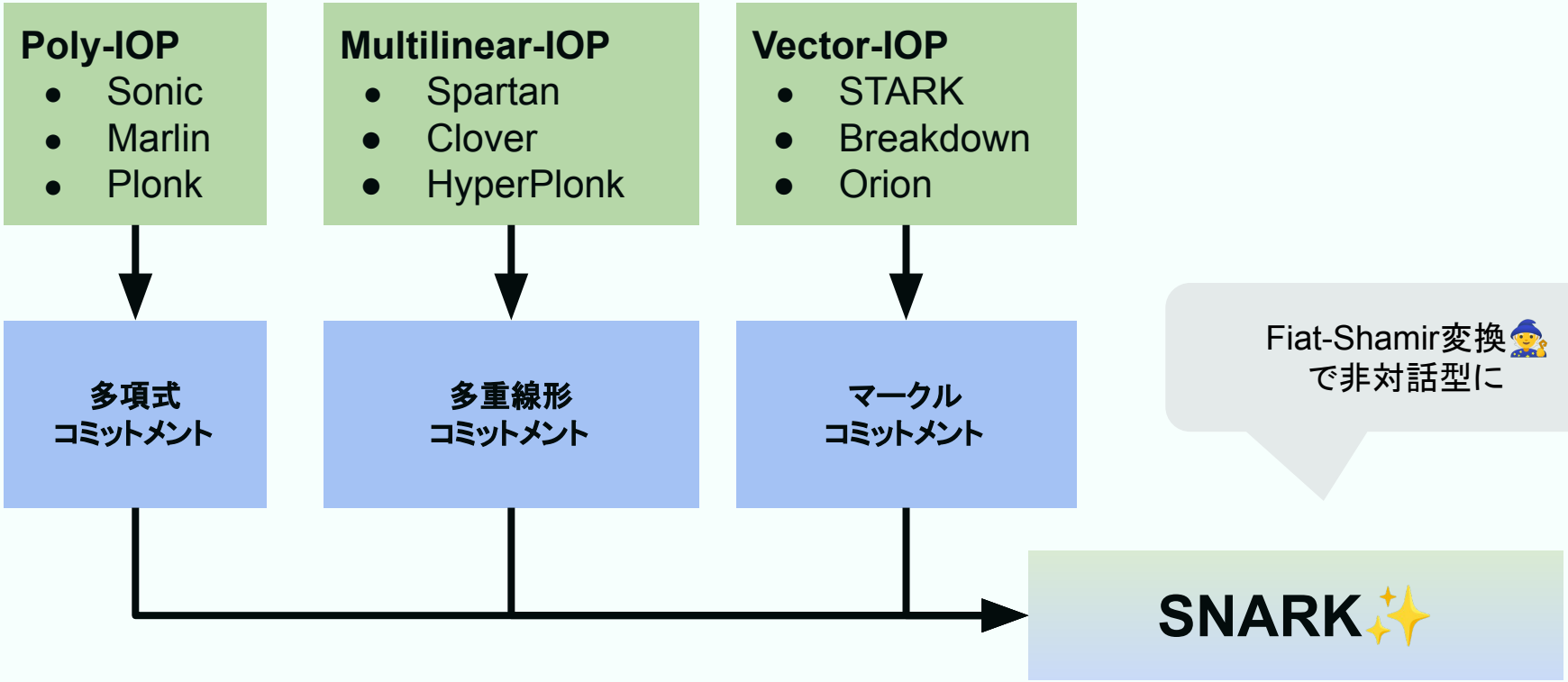
明日の天気は？

🌤️

インタラクティブオラクルプルーフ (IOP)

- 証明者と検証者が対話しながら C(x,w)=0を証明する証明システム
- 検証者はオラクルにアクセスできる
  - PCSなどで代替される

IOP図鑑


Poly-IOP
Sonic
Marlin
Plonk
Multilinear-IOP
Spartan
Clover
HyperPlonk
Vector-IOP
STARK
Breakdown
Orion
多項式
コミットメント
多重線形
コミットメント
マークル
コミットメント
SNARK✨
Fiat-Shamir変換🧙
で非対話型に

対話型証明をSNARKに

Fiat-Shamir変換

対話型証明 → 非対話型証明

SNARKの実用的な構成

多項式に変換されて IOPで証明！

ドメイン固有言語プログラム
Circom, Noir, …

```
pragma circom 2.1.8;

include "./node_modules/circomlib/circuits/comparators.circom";
include "./node_modules/circomlib/circuits/poseidon.circom";

template UnsafePoseidon(n) {
    signal input in;
    signal output out;

    component n2b = Num2Bits(n);
    component b2n = Bits2Num(n);
    component phash = Poseidon(1);

    n2b.in <== in;
    for (var i = 0; i < n; i++) {
        b2n.in[i] <== n2b.out[i];
    }

    phash.inputs[0] <== b2n.out;
    phash.out ==> out;
}

component main = UnsafePoseidon(254);
```

SNARKフレンドリな形式
Circuit, R1CS, …, EVM byte code

A		B		C	
1	5	1	1	1	0
3	0	3	0	3	0
35	0	35	0	35	1
9	0	9	0	9	0
27	0	27	0	27	0
30	1	30	0	30	0

35 * 1 - 35 = 0

証明システム

x,w

π

まとめ

- ゼロ知識証明は主張が正しいことを主張に関する情報を伝えずに証明する
- SNARKは回路C(x,w)=0を簡潔に検証可能にする
- zkSNARKは「多項式コミットメントスキーム」と「インタラクティブオラクルプルーフ」を組み合わせて構成される
- おすすめの補助教材
  - ZK MOOC
  - ZK Whiteboard Sessions

参考資料

- https://rdi.berkeley.edu/zk-learning/assets/Lecture2-2023.pdf
- https://www.docswell.com/s/linoscope/582D91-2025-04-05-174750#p12

演習問題

1) zkSNARKの具体的なユースケースを自分で一つ考えて、p.23にある方式のうちどれを使うべきか理由とともに説明してください
2) 実用化されているZKアプリケーションを一つ見つけて、以下の3つのドメインに何が採用されているのかURLとともに答えてください
    a) ドメイン固有言語
    b) SNARKフレンドリな形式
    c) バックエンド証明器
3) (+α問題) 2で採用されている方法にはどんな特徴があるか説明してください

ヒント: アプリケーションに困ったら ここや補助教材を参考にしてみてね。特徴は AIに聞いてもいいよ。

ZK Tokyo

Thank you!