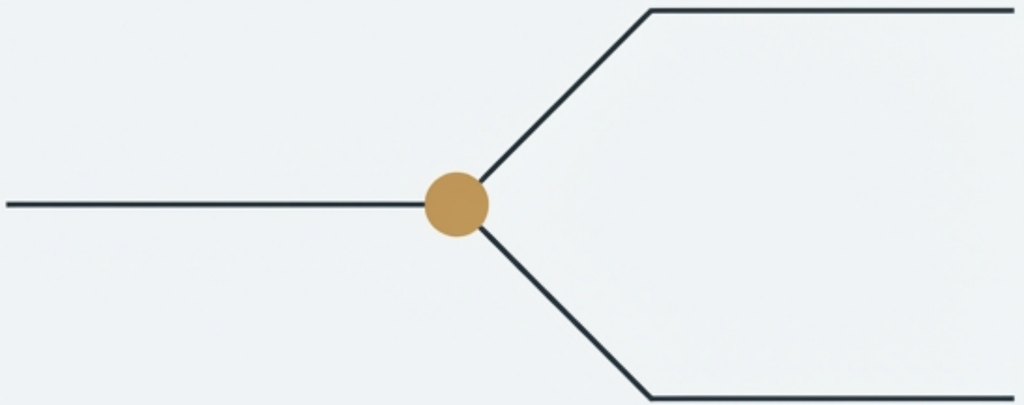
分岐補題 (Forking Lemma) の完全理解

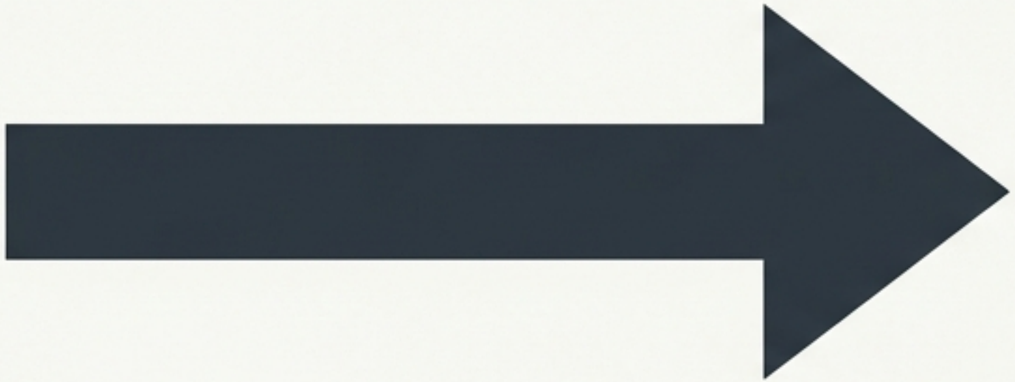
ランダムオラクルモデルにおけるた存在的偽造の困難性と、根底にある数学的難問との結びつきを解き明かす。



署名の偽造が「不可能」であることをどう証明するか？

暗号理論における証明の基本論理：
「もし偽造ができたとすると、もっと難しい問題を解くことも（無視できない確率で）可能になる」

つまり、偽造の成功を、因数分解や離散対数問題といった「絶対に解けない数学的難問」の突破と結びつける背理法です。



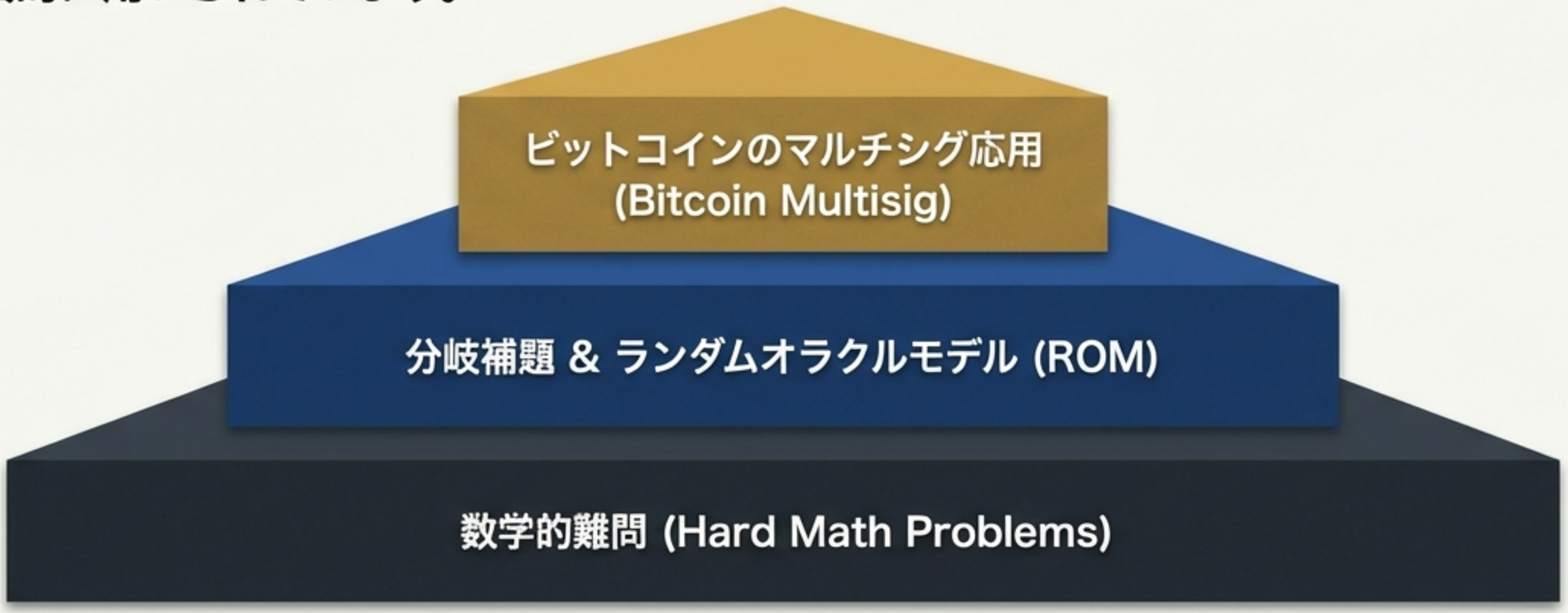
If: 署名の偽造

Then: 数学的難問の突破

現代暗号とビットコインを支える数学的基盤

分岐補題は、ランダムオラクルモデル（ROM）を採用する署名形式の安全性を証明する中核的な定理です。

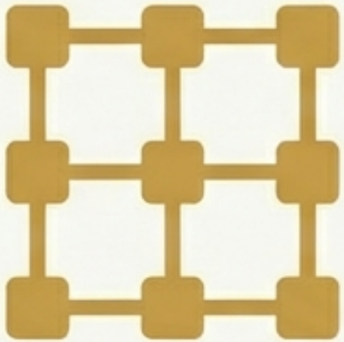
近年では、ビットコインネットワークにおける様々なマルチシグ（多重署名）応用の安全性証明にも直接的に用いられています。



偽造者とのゲームに登場する4つの主要パラメータ

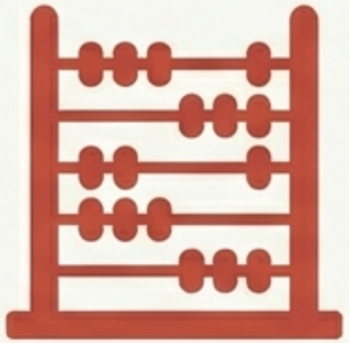
x

公開鍵などの
パブリックパラメータ



H

ハッシュ関数（ランダムオラクル）の空空間（要素数 h ≥ 2）



q

偽造の試行回数
（ランダムオラクルへのクエリ回数）

A

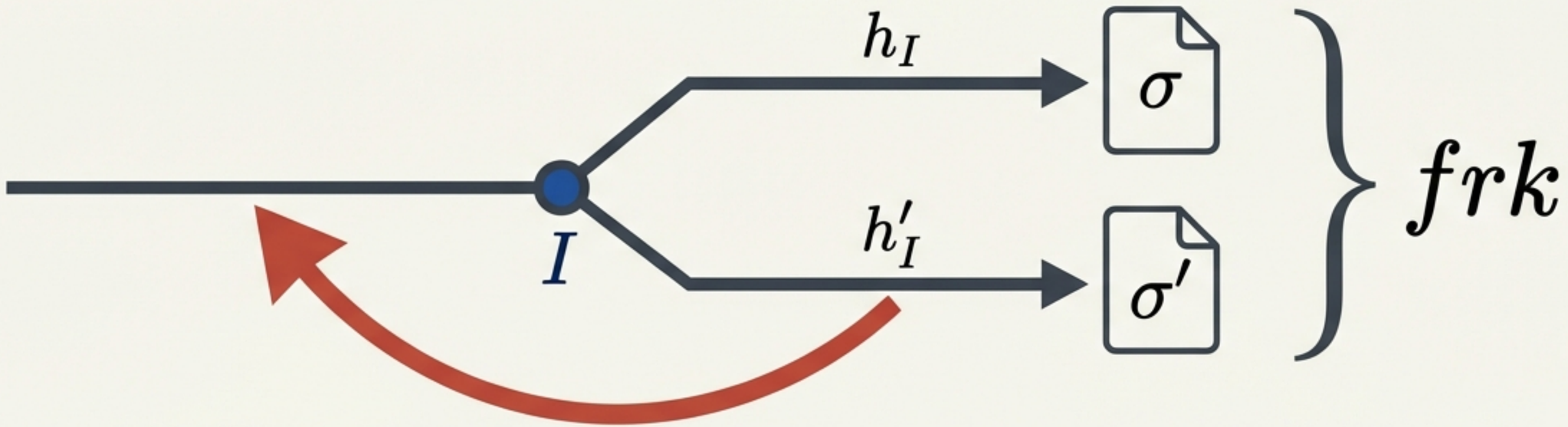
攻撃者を模した
ランダムアルゴリズム

acc: アルゴリズム A が存在的偽造に成功する確率（受理確率）

時間を巻き戻し、別の現実を分岐させるアルゴリズム

分岐アルゴリズム $FA(x)$ の動作：

1. 乱数シード ρ でアルゴリズム A を実行し、偽造に成功する点 I を記録。
2. 状態を I の直前まで巻き戻す。
3. 成功点 I のハッシュ関数だけを別のもの ($h_I \neq h'_I$) にすり替える。
4. 再度実行し、同じ点 I で連続成功する確率を frk と定義する.



偽造成功率と分岐成功率を結ぶ中核的な不等式

一般分岐補題が示す圧倒的な制約：

$$acc \leq \frac{q}{h} + \sqrt{q \cdot frk}$$

偶然ハッシュが当たる
ベースラインの確率

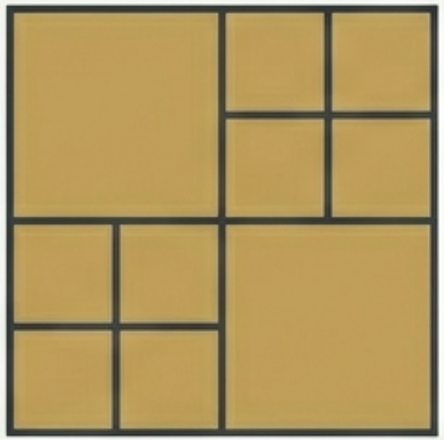
分岐成功から得られる
偽造確率の上限

偽造確率（acc）は、単なる「偶然の的中」と「分岐アルゴリズムの成功確率の平方根」の和によって、絶対的な上限が定められます。

期待値の性質が導く「平方根」の数学的直感

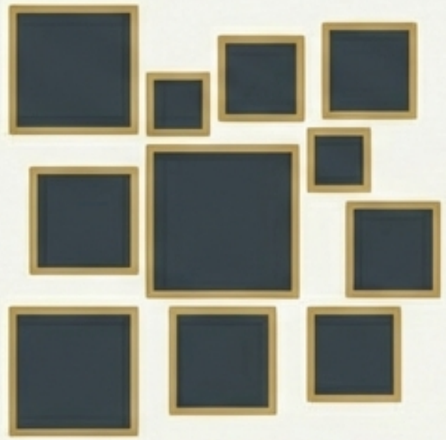
なぜ式に平方根が現れるのか？

連続して2回偽造に成功する確率は、1回の試行における確率変数 X_i を用いて期待値の計算に落とし込めます。
確率論の基本性質 $\sum E[X_i^2] \geq \sum E[X_i]^2$ より、期待値の二乗の和で下から抑え込むことができるため、逆算すると平方根が現れます。



$\sum E[X_i^2]$（期待値の二乗の和）

$\geq$

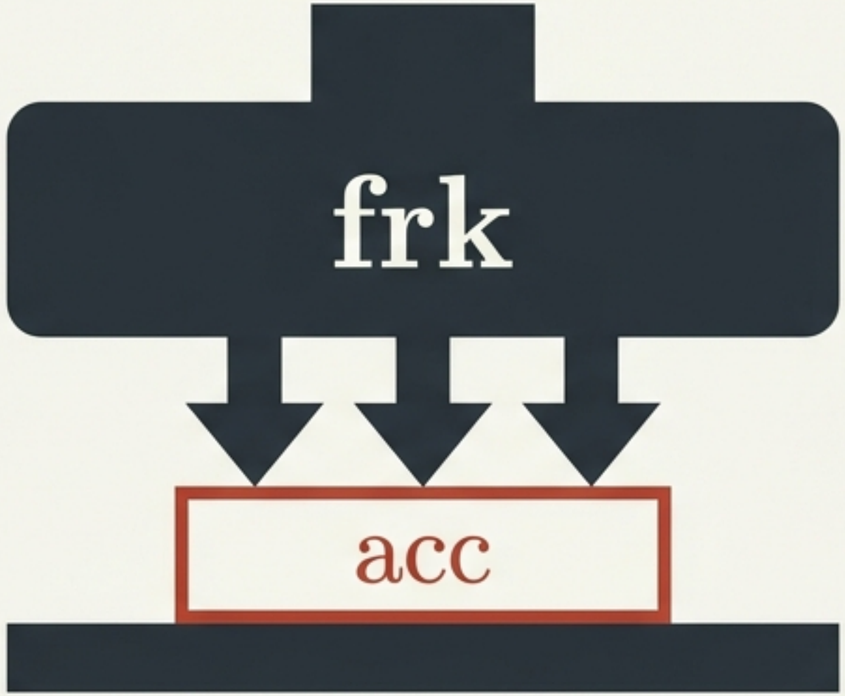


$\sum E[X_i]^2$（二乗の期待値の和）

2回の連続成功が保証する、偽造の圧倒的困難さ

理論の要約：

- frk（2回連続の成功）は、感覚的にも acc（1回の成功）の二乗に比例します。
- 逆に言えば、acc は frk の平方根によって「上から抑え込まれて」います。
- もし frk を「絶対に起きないレベルの極小の確率」にできれば、acc も必然的にゼロに近づきます。



抽象から具体へ：シュノア署名における証明の可視化

では、実際に分岐補題によって「2つの有効な偽造署名」が生成されたとき、何が起きるのでしょうか？

シュノア署名を例に、偽造者が「離散対数問題」の答えを自ら暴露してしまう過程を追います。

シュノア署名の舞台設定とパラメータの定義

公開パラメータ: 素数 p, 位数 q, 生成元 g,
公開鍵 y $(y = g^x \bmod p)$

秘密のパラメータ: 秘密鍵 x

偽造署名に共通のランダム値: $R = g^r$
(偽造者は R を知っているが r は不明)

同じ乱数、異なるハッシュから生まれた2つの偽造署名

分岐補題により、共通の R を持つ2つの偽造署名 (e_1, t_1) と (e_2, t_2) が得られます。
分岐の性質上、ハッシュ値は異なります: e_1 ≠ e_2

$$R$$

署名1:

$$e_1 = H_1(m; g^{t_1} y^{e_1})$$

$$R$$

署名2:

$$e_2 = H_2(m; g^{t_2} y^{e_2})$$

$$e_1 \neq e_2$$

2つの偽造を衝突させ、方程式を解き明かす

両方の署名は検証をパスするため、共通の R を介して等式で結ばれます。
項を整理してまとめます：

$$g^{t_1} y^{e_1} = R = g^{t_2} y^{e_2} \bmod p$$

↓

$$g^{t_2 - t_1} = y^{e_1 - e_2} \bmod p$$

偽造の代償：秘密鍵の完全な抽出

ここで公開鍵 $y = g^x$ を代入し、秘密鍵 x について解きます。

$$g^{t_2 - t_1} = g^{x(e_1 - e_2)}$$

2つの偽造データから、完全に秘密鍵 x が導出されました。

離散対数問題が解かれた瞬間です！

$$\boxed{x} \equiv (e_1 - e_2)^{-1}(t_2 - t_1) \bmod q$$

抽出された秘密鍵

離散対数問題の壁が、署名の安全性を完全に担保する

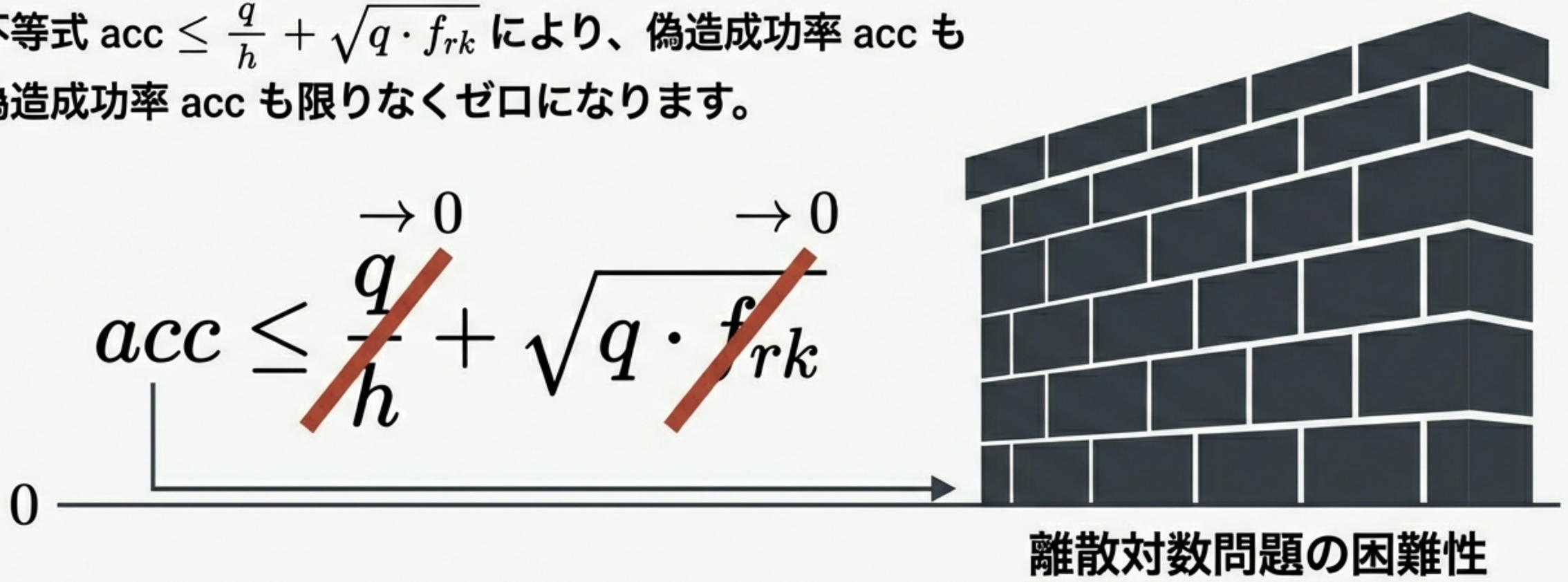
現実には、離散対数問題を解くことは計算量的に不可能です。

したがって、$f_{rk} \approx 0$ となります。十分大きなハッシュ空間 (h) を使えば $\frac{q}{h} \approx 0$ となり、

不等式 acc $\leq \frac{q}{h} + \sqrt{q \cdot f_{rk}}$ により、偽造成功率 acc も

偽造成功率 acc も限りなくゼロになります。

$$acc \leq \overset{\to 0}{\cancel{\frac{q}{h}}} + \sqrt{q \cdot \overset{\to 0}{\cancel{f_{rk}}}}$$



分岐補題が示す「安全性の証明」のエレガンス

直感的に理解しづらい分岐補題ですが、その本質は「偽造者をタイムトラベルさせ、自らの矛盾で秘密密を暴露させる」という極めてエレガントな論理構造にあります。

シュノア署名だけでなく、ElGamal署名など、ROMを利用する多くのプロトコルにこの定理は応用されています。

参考文献：Pointcheval & Stern (2000), Security Arguments for Digital Signatures and Blind Signatures