最短1ラウンド署名を実現する技術：類群を用いた2ラウンド閾値ECDSAの深層

社内技術勉強会

本日のアジェンダ

1. THE GOAL: 2ラウンド閾値ECDSAプロトコル

我々が目指す最終的な成果物とその構造を理解する

2. THE ENGINE: 非対話型積和変換 (NIM) アルゴリズム

プロトコルを駆動する中心的な「ブラックボックス」の仕組みを解き明かす

3. THE MAGIC: 類群の数学と剰余類ラベル関数φ

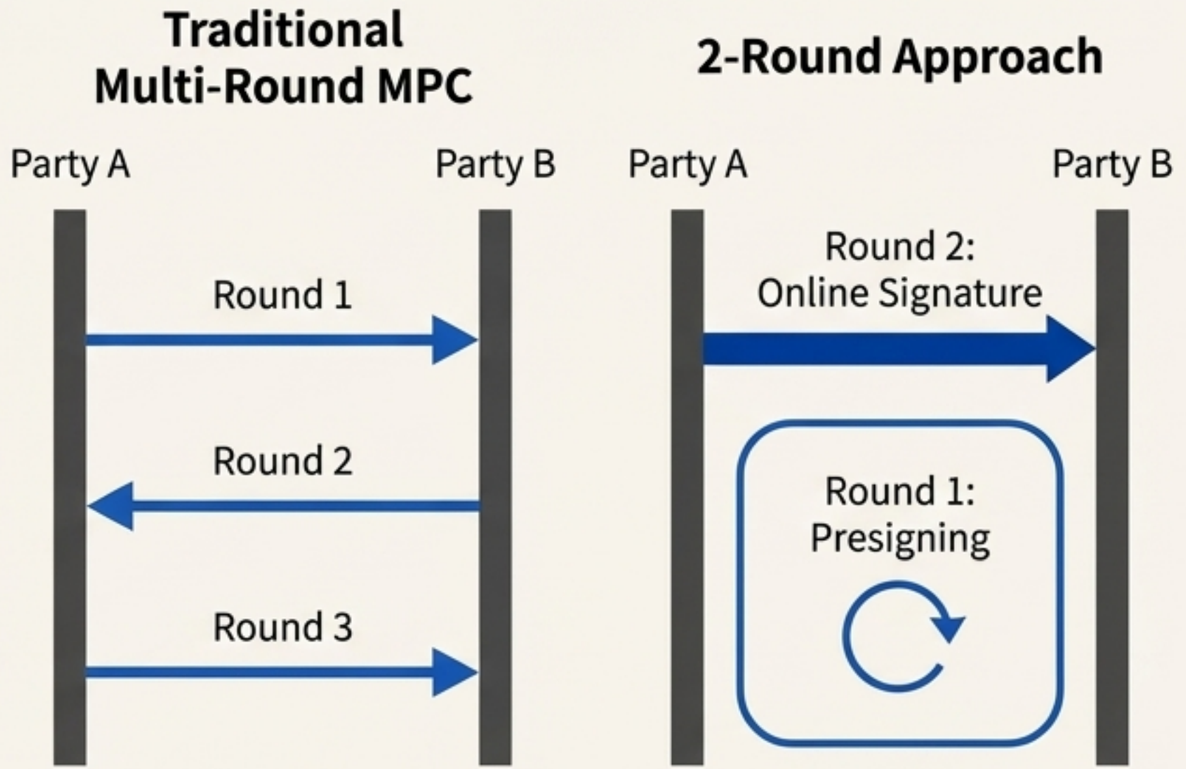
NIMを可能にする独創的な数学的発想の核心に迫る

The Challenge: なぜラウンド数を減らすことが重要なのか？

従来のMPCベースのECDSAでは、複数回の通通信ラウンドが必要であり、これがパフォーマンスのボトルネックとなっていた。

特にオンラインフェーズでの通信を最小限に抑えることが、高速な署名生成の鍵となる。

Goal: 既存の3ラウンド以上のプロトコルに対し、オンライン通信を実質1ラウンドにまで削減することを目指す。



> 本手法は、非標準的な暗号学的仮定（類群上のDDH-CL, DXDH-CL）に依存することで、この効率化を達成している。標準的な仮定を用いる3ラウンドの手法[^7]も存在する。

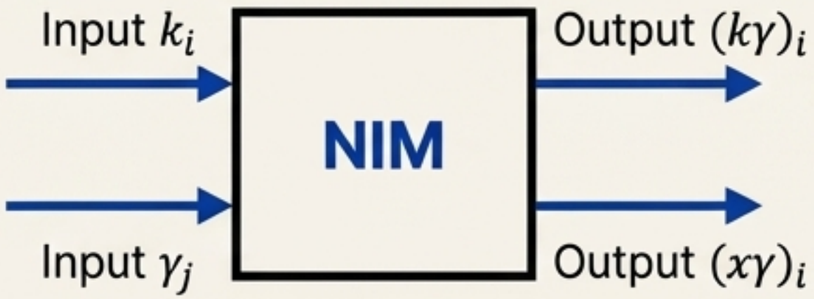
The Goal: 2ラウンド閾値ECDSAプロトコルの全体像

Round 1: Presigning (事前計算)

各参加者iは乱数 k_i, γ_i を選択し、g^{k_i} を公開。

各ペア (i,j) は **NIMアルゴリズム** を用いて $k_i * \gamma_j$ と $x_i * \gamma_j$ の加法シェアを非対話で計算。

結果、各参加者 i は $k\gamma$ と $x\gamma$ の加法シェア $(k\gamma)_i, (x\gamma)_i$ を保持する。



Round 2: Online Signature (オンライン署名)

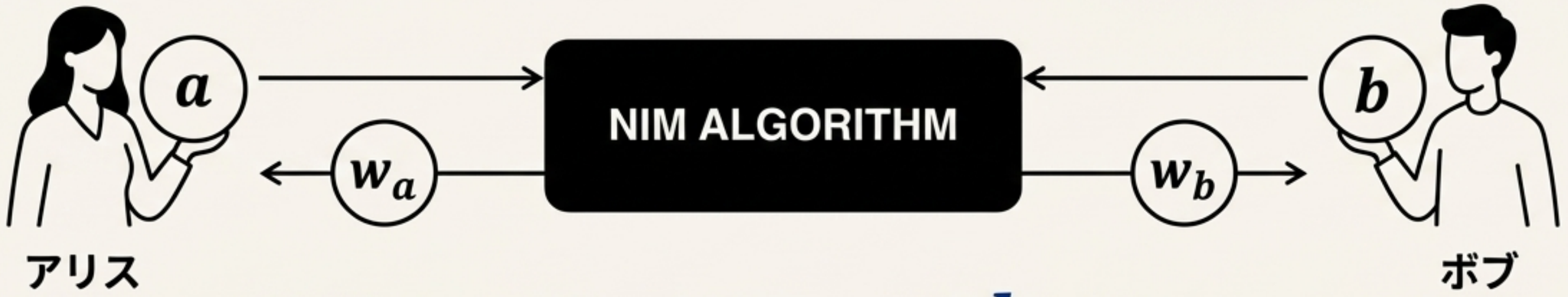
メッセージ m が確定後、$R=g^{zk+y}$ を計算し、r を公開。

各参加者 i はシェアを用いて $\sigma_i = m\gamma_i + r(x\gamma)_i$ と $\delta_i = z(k\gamma)_i + y\gamma_i$ を計算し送信。

全員の値を集約し $\sigma = (\sum\delta_i)^{-1} * (\sum\sigma_i)$ を計算して署名が完成。

プロトコル中の乗算 $(k_i * \gamma_j, x_i * \gamma_j)$は、NIMという「魔法の箱」によって、通信を必要としない加算に変換される。

The Engine: 非対話型積和変換 (NIM)



$$w_a + w_b = ab$$

Core Objective:
アリスは秘密の値 a を、ボブは秘密の値 b を持っている。
目標:** 最小限のやり取りで、積 ab の加法シェア w_a, w_b を計算したい。すなわち、$w_a + w_b = ab$ を満たす値を、それぞれがローカルで計算できるようにする。

Context
このアルゴリズムが、前述の $k_i * \gamma_j$ のような計算を、各パーティが独立して行えるようにする鍵である。

NIMアルゴリズムの動作ステップ

h_0, h_1, f は共有された群の生成元。

アリス (Alice)

Input: 秘密 a，乱数 r

Send to Bob: $d = h_0^r * h_1^a$

Local Compute: $Z_A = e_0^r * e_1^a$

$= (h_0^s)^r * (f^b * h_1^s)^a$

$= h_0^{rs} * f^{ab} * h_1^{as}$

ボブ (Bob)

Input: 秘密 b，乱数 s

Send to Alice: $(e_0, e_1) = (h_0^s, f^b * h_1^s)$

Local Compute: $Z_B = d^s$

$= (h_0^r * h_1^a)^s$

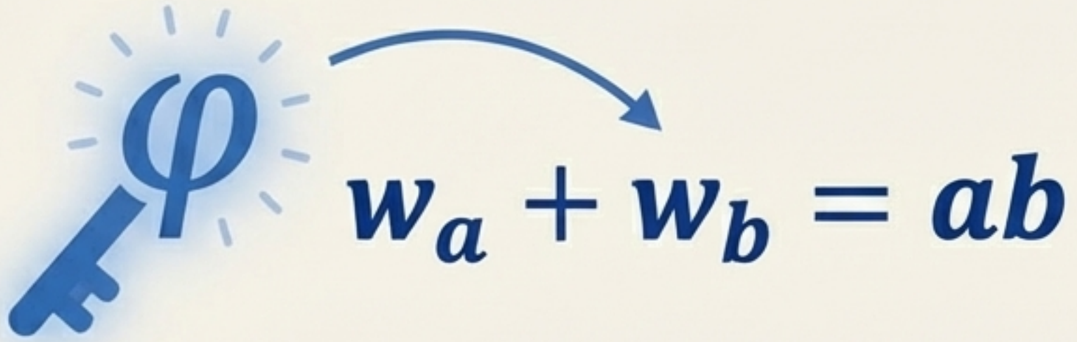
$= h_0^{rs} * h_1^{as}$

アリスとボブが計算した値の比を取ると、乱数項が相殺される。

$$Z_A / Z_B = (h_0^{rs} * f^{ab} * h_1^{as}) / (h_0^{rs} * h_1^{as}) = f^{ab}$$

これにより、両者は積 ab が指数部に乗った共通の群要素 f^{ab} を得た。
しかし、ここからどうやって加法シェアを取り出すのか？

f^{ab} から加法シェアへ：最後のピース



我々は f^{ab} という形で積 ab を含む群要素を導出した。しかし、ab を直接得るためには離散対数問題を解く必要があり、これは計算上困難である。我々が必要なのは ab そのものではなく、$w_a + w_b = ab$ を満たすシェア w_a, w_b である。

ここで登場するのが、イデアル類群の特殊な性質を利用した **剰余類ラベル関数**（Coset Label Function）ϕ である。この関数 ϕ が、困難な離散対数問題を回し、指数部分の値をシェアとして抽出する「魔法の杖」の役割を果たす。

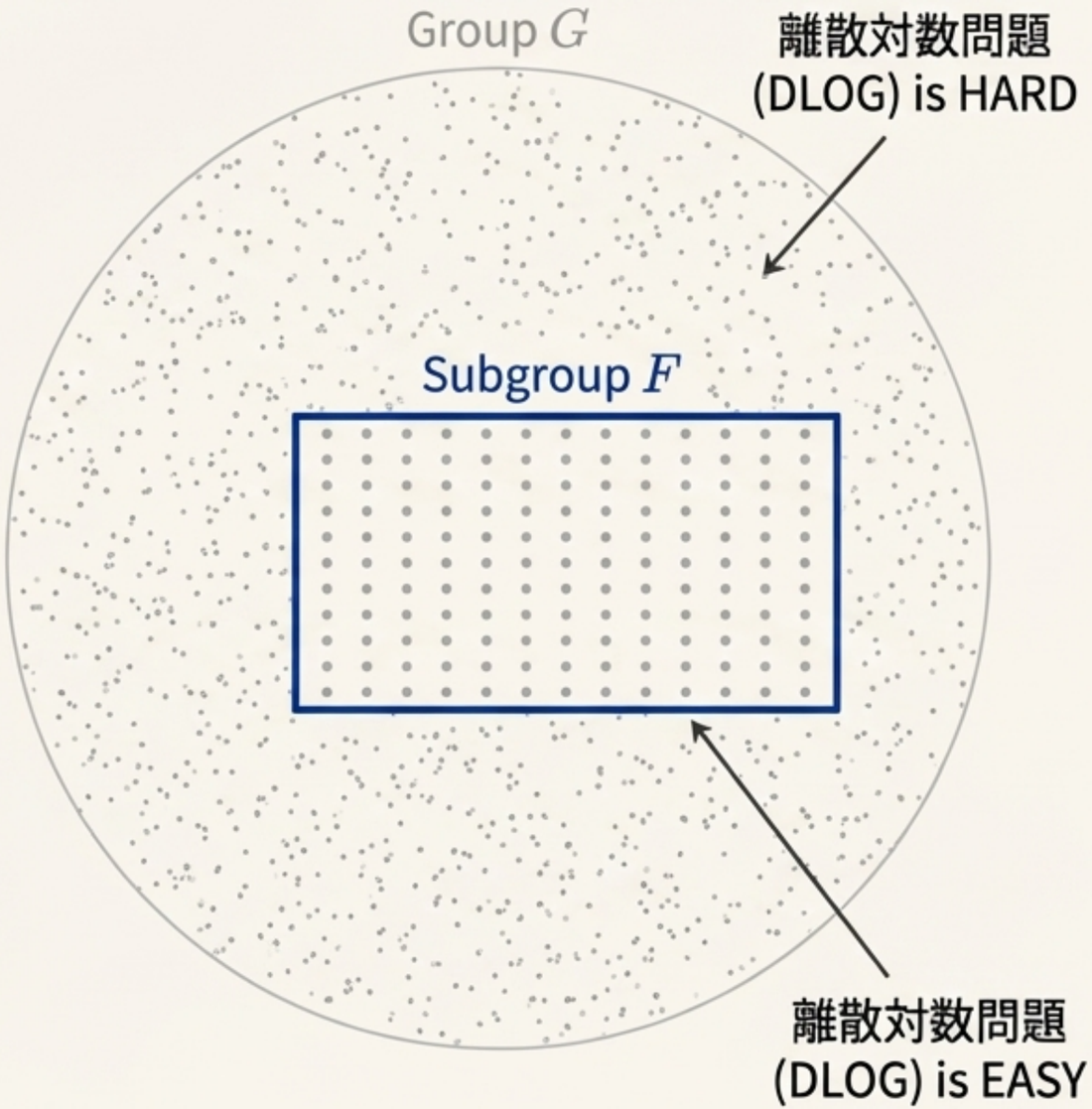
The Magic: イデアル類群の力

Why Class Groups?:

- 類群は、暗号学的に非常に興味深い構造を持つ。
- **Key Property**: 全体としては離散対数問題が困難な巨大な群 G の中に、離散対数問題が**容易に解ける**特殊な部分群 F が存在する。
- この「困難な問題」と「容易な問題」の共存が、NIMアルゴリズムの核となるトリックを可能にする。

Additional Benefit:

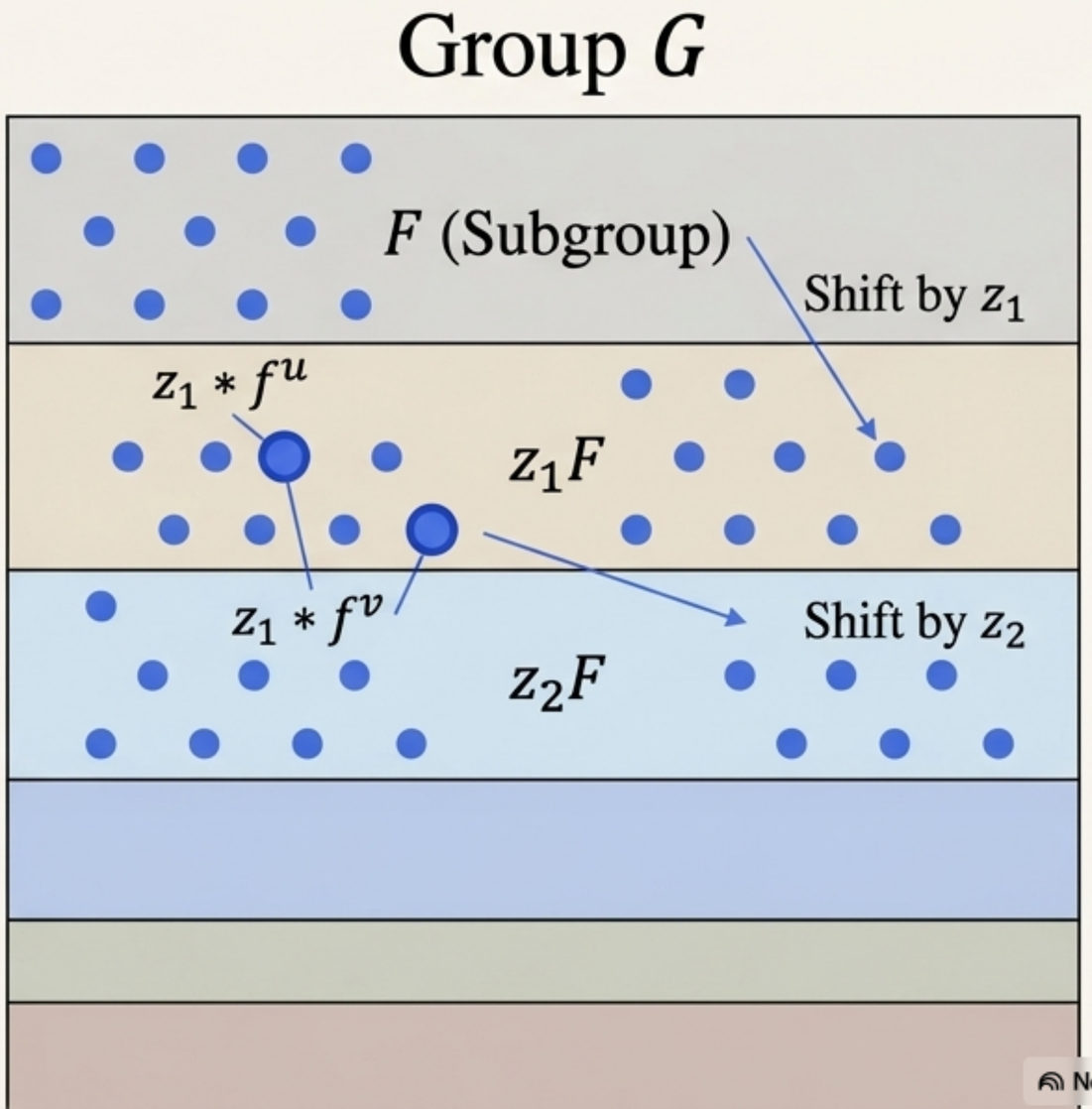
- 類群を用いることで、トラステッドセットアップが不要になる。これは、ペイエ暗号などの他のアプローチに対する大きな利点である。



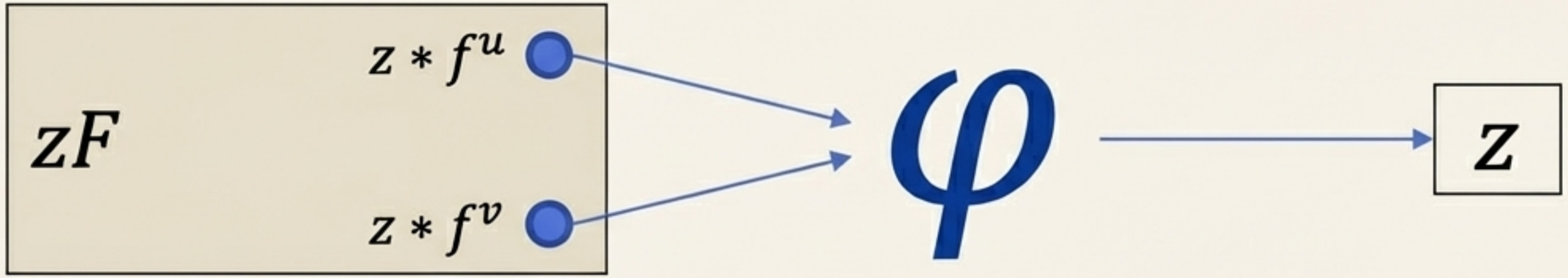
核心コンセプト：剰余類 (Coset)

Definition:
群 G とその部分群 F があるとする。
ある元 $z \in G$ に対し、剰余類 zF は、F の全要素を z で「シフト」した集合である。
$zF = \{z * f \mid f \in F\}$

Intuition:
群 G は、互いに素な剰余類の集まりとして完全に分割できる。
同じ剰余類に属する要素は、$z * f^u$ と $z * f^v$ のように、共通の「代表元 (representative)」z と、部分群 F の要素 f^u, f^v の積で表現できる。



魔法の杖：剰余類ラベル関数 φ



φ は、ある要素が属する剰余類の「ラベル」あるいは「代表元」を一意に返す関数である。

入力が同じ剰余類 zF に属する要素であれば、出力は常に同じ代表元 z となる。

$$\varphi(z * f^u) = z \qquad \varphi(z * f^v) = z$$

アリスが $z * f^u$ を、ボブが $z * f^v$ を持っている場合でも、それぞれが φ を適用すれば、e、通信なしで共通の値 z に合意できる。

φの適用：NIMアルゴリズムの完成

Recall: アリスは Z_A を、ボブは Z_B を計算済み。$Z_A/Z_B = f^{ab}$ であるため、Z_A と Z_B は同じ剰余類に属する。

1. **ラベル取得 (Get Label)**
   Alice: $l_A \leftarrow \varphi(Z_A)$
   Bob: $l_B \leftarrow \varphi(Z_B)$
   φの性質により、$l_A = l_B$ となる共通のラベル l が得られる。

2. **剰余類部分を消去 (Isolate Subgroup Element)**
   Alice: $X_A \leftarrow Z_A * l^{-1}$
   Bob: $X_B \leftarrow Z_B * l^{-1}$
   これにより、X_A と X_B は「DLOGが容易な」部分群 F の要素となる。

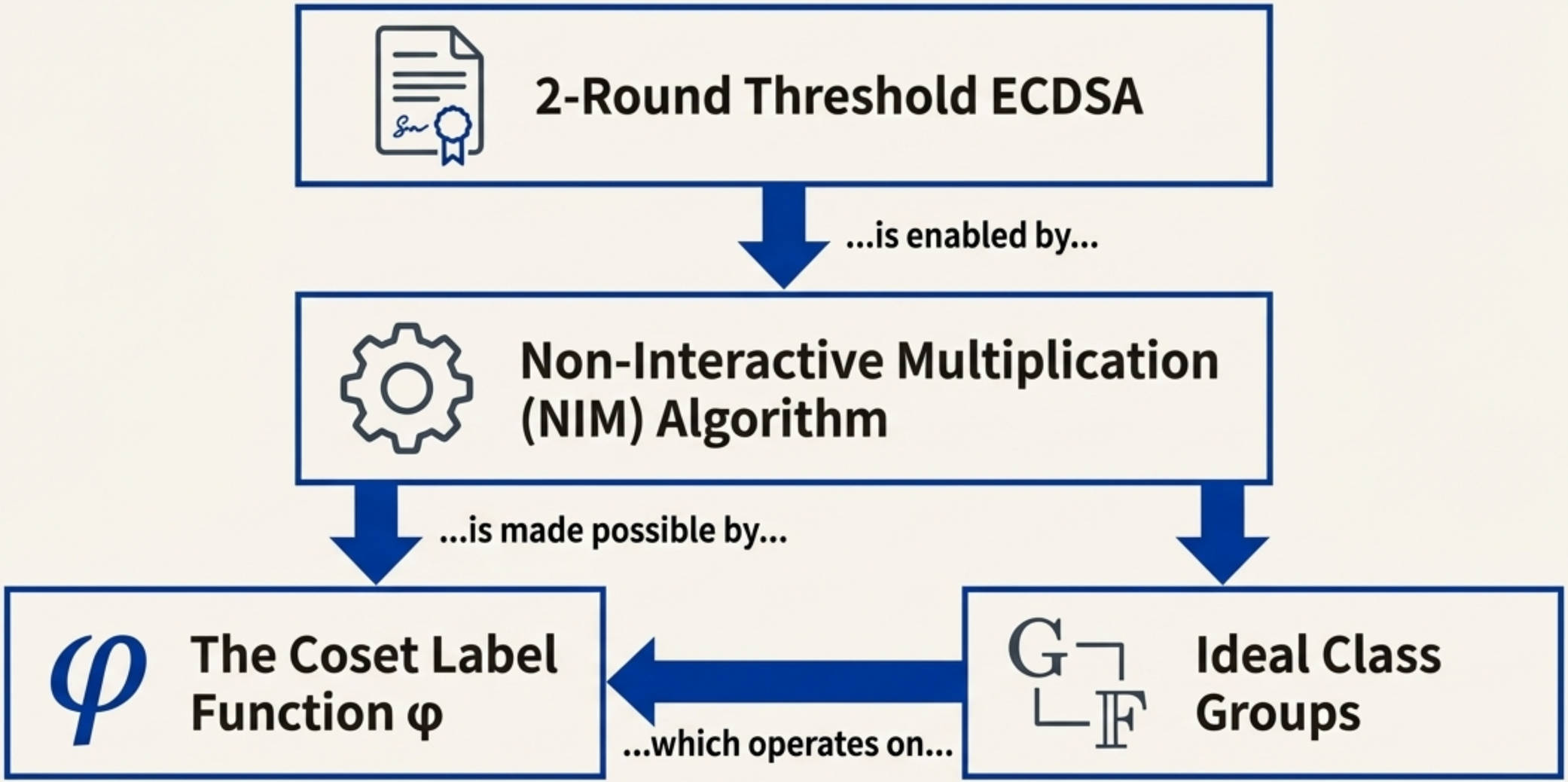
3. **指数を計算 (Compute Exponent)**
   Alice: $w_a \leftarrow \log_f(X_A)$
   Bob: $w'_b \leftarrow \log_f(X_B)$

4. **シェアを確定 (Finalize Shares)**
   アリスのシェア: w_a
   ボブのシェア: $w_b = -w'_b$

$$
\begin{aligned}
w_a + w_b &= \log_f(X_A) - \log_f(X_B) \\
&= \log_f(X_A/X_B) \\
&= \log_f((Z_A/l)/(Z_B/l)) \\
&= \log_f(Z_A/Z_B) \\
&= \log_f(f^{ab}) \\
&= ab
\end{aligned}
$$

これにより、$w_a + w_b = ab$ が達成された。

全体像の再確認：技術の階層構造



効率的な**2ラウンドECDSA**は、非対話での積和変換を可能にする**NIMアルゴリズム**によって実現される。
そのNIMアルゴリズムの心臓部には、**イデアル類群**の特殊な構造を利用した**剰余類ラベル関数φ**が存在する。

まとめとトレードオフ

利点

- ✓ **高速な署名 (Fast Signatures)**：オンラインフェーズが実質1ラウンドであり、通信のボトルネックを解消。
- ✓ **シンプルなプロトコル (Simple Protocol)**：複雑な積和変換の仕組みがNIMに集約されており、ECDSAプロトコル自体の構造は非常に見通しが良い。
- ✓ **トラステッドセットアップ不要 (No Trusted Setup)**：類群を用いることで、信頼できる第三者による初期設定が不要となる。

欠点・考慮事項

- ⚠ **非標準的な暗号学的仮定 (Non-Standard Assumptions)**：安全性が、楕円曲線暗号などで用いられる標準的な仮定ではなく、類群上のDDH-CLやDXDH-CLといった比較的新しい仮定に依存する。
- ⚠ **パフォーマンス**：類群の演算は、特定の条件下で楕円曲線上の演算よりもコストが高くなる可能性がある。

最終考察：類群暗号の正当性

- 「イデアル類群」は馴染みが薄いかもしれないが、その研究は楕円曲線暗号と同様に1980年代から続く歴史を持つ暗号ファミリーである。
- その安全性は、楕円曲線と同様に、複雑な群構造における離散対数問題の困難性に根差している。
- 類数計算（＝類群の元の数を数えること）の困難性は、19世紀初頭のガウスの時代から認識されてきた歴史的な難問であり、その計算困難性が暗号の安全性の根拠となっている。

どの仮定が「より保守的」かを一概に決めることは困難であり、多様な数学的難問に安全性を依拠させることは、暗号学全体の堅牢性に貢献する。