Computer Security Symposium 2025
27-31 October 2025

非対話ブラインド署名の構成可能性について

山村 和輝[1,a)]

概要：本稿では、非対話ブラインド署名 (Eurocrypt'23) における通常モデルでの構成可能性について考察する。特に偽造不可能性から非対話仮定へ帰着するブラックボックス帰着が存在するのか議論する。

キーワード：ブラインド署名

On Non-Interactive Blind Signatures

Kazuki Yamamura[1,a)]

Abstract: In this work, we study the limits of constructing non-interactive blind signatures.

1. はじめに

ブラインド署名は、Chaum によって導入された暗号学における基本的な原始概念であり、電子投票 [3]、電子キャッシュ [4], [5]、匿名認証情報 [2] など数多くの応用を有するデジタル署名である。具体的には、ブラインド署名は、署名鍵を保持する署名者とメッセージを保持する受信者との間の対話型プロトコルであり、署名者が署名対象のメッセージを知らずに受信者が署名を生成することを可能とする。

ブラインド署名は、*blindness* と 偽造不可能性 という二つの主要な安全性要件を満たす必要がある。直感的には、blindness とは署名者がプロトコル実行と生成されるメッセージ・署名ペアとの間にいかなる関連を認識できないことを保証し、偽造不可能性とは受信者が署名者との対話なしに有効な署名を生成できないことを保証するものである。

すなわち、ブラインドは本質的に対話通信を行い対話中に受信者が状態を保持する必要がある。しかし、Hanzlik [6] は、署名者と受信者との間のオンラインでの対話通信を必要とせずにブラインド署名を生成できる、非対話ブラインド署名（non-interactive blind signature, NIBS）を導入した。NIBS の特徴として、標準的なブラインド署名では受信者がメッセージを指定できるのに対し、NIBS の場合、受信者および署名者の双方にとって予測不可能である点にある。とはいえ、この性質は Privacy Pass [9]、内部告発システム、抽選システム、電子コインのエアドロップ [8] といった多くの応用が可能であり、この予測不可能性はむしろ望ましい場合さえある。

ここで、$\mathsf{NIBS} := (\mathsf{KeyGen}, \mathsf{RKeyGen}, \mathsf{Issue}, \mathsf{Obtain}, \mathsf{Verify})$ の署名生成の流れを簡単に紹介する。KeyGen および RKeyGen は、それぞれ署名者と受信者の鍵生成アルゴリズムである。これは実行に先立ち、（標準的なブラインド署名と異なり、）署名者が秘密鍵／公開鍵ペア $(\mathsf{sk}, \mathsf{pk})$ を保持するだけでなく、受信者も自身の秘密鍵／公開鍵ペア $(\mathsf{rsk}, \mathsf{rpk})$ を生成・保持する必要がある。まず、Issue フェーズおいて、署名者は受信者の公開鍵 rpk と乱数メッセージを決定的に指定するノンス nonce に対して、事前署名である psig を生成する。$((\mathsf{psig}, \mathsf{nonce}) \leftarrow \mathsf{Issue}(\mathsf{sk}, \mathsf{rpk}))$. 次に、Obtain フェーズにおいて、受信者は $(\mathsf{psig}, \mathsf{nonce})$ を受け取り、自身の秘密鍵 rsk を用いてランダムメッセージ m に対するブラインド署名 sig を生成する。$((\mathsf{m}, \mathsf{sig}) \leftarrow \mathsf{Obtain}(\mathsf{rsk}, \mathsf{pk}, (\mathsf{psig}, \mathsf{nonce})))$. 最後に、検証フェーズにおいて、この署名は署名者の公開鍵 pk によって検証可能である $(1 = \mathsf{Verify}(\mathsf{pk}, \mathsf{m}, \mathsf{sig}))$. ここで重要なのは、受信者の公開鍵 rpk が事前に公開されていなければならないという点である。例えば、各受信者の公開鍵が既存の PKI に登録されているならば、署名者は受

[1] NTT 社会情報研究所
NTT Social Informatics Laboratories
[a)] kazuki.yamamura.by@hco.ntt.co.jp

信者と対話通信をすることなく事前署名を発行することが可能となる。

標準的なブラインド署名と同様に、NIBS も偽造不能性と blindness を満たすことが要求される。偽造不能性ゲームにおいて、攻撃者は任意に指定した受信者公開鍵に対する事前署名 - ノンスのペアを返すオラクルにアクセスできる。最終的に攻撃者は、オラクルへのクエリ回数を超える有効な署名を出力しなければならない。一方、 NIBS における blindness は、*recipient blindness* と *nonce blindness* という二つの異なる性質から構成される。*recipient blindness* は、メッセージ - 署名ペアが受信者の公開鍵に関する情報を漏らさないことを保証し、*nonce blindness* はそれらがノンスに関する情報を漏らさないことを保証する。形式的には、recipeint blindness ゲームでは、攻撃者は二つの正しく生成された受信者公開鍵 rpk_0, rpk_1 を与えられ、二つの事前署名 - ノンスのペア $(\mathsf{psig}_0, \mathsf{nonce}_0)$ および $(\mathsf{psig}_1, \mathsf{nonce}_1)$ を出力する。これらはチャレンジャーによってメッセージ - 署名ペア $(\mathsf{m}_0, \mathsf{sig}_0)$ および $(\mathsf{m}_1, \mathsf{sig}_1)$ が生成され、攻撃者は、それらがランダムに並べ替えられた状態で与えられ、どの受信者が各ペアを生成したかを識別しなければならない。ノンス盲目性ゲームでは、攻撃者は一つの受信者公開鍵 rpk のみを与えられ、事前署名 - ノンスのペアに用いられたノンスを識別しなければならない。どちらの blindness ゲームにおいても中止は考慮されず、署名が完成できなかった場合、攻撃者には $(\bot, \bot)$ が与えられる。

上記の blindness の性質は [6] で導入され、本論文では *weak blindness* と呼ぶ。しかし、多くの応用において *weak blindness* では不十分であり、したがって NIBS は [1] で導入されたより強力な blindness を満たすことが求められる。本論文ではこれを *strong blindness* と呼び、複数の事前署名が発行される状況においても strong recipient blindness と strong nonce blindness の両方を満たすことが要求される。

Strong blindness ゲームにおいて、攻撃者は受信者の秘密鍵に対する Obtain クエリという形でオラクルアクセスを与えられる。この Obtain オラクルは、署名者の公開鍵と事前署名 - ノンスのペアを入力として受け取り、Obtain アルゴリズムを用いて対応するメッセージ - 署名ペアを正しく完成させて返す。攻撃者がゲームに自明に勝利することがないように、攻撃者は二つのチャレンジ事前署名 psig_0, psig_1 またはそれらに対応するノンス nonce_0, nonce_1 に対して Obtain クエリを行うことは禁止される。本論文の結果はこの Strong blindness についても焦点を当てる。

ここで、既存の NIBS について述べる。Hanzlik の構成 [6] に続き、複数の NIBS が提案されている [1], [7], [10], [13] が、我々の知る限り、[10] を除くすべての NIBS は通常モデルではない形で構成されており、ランダムオラクルモデル（ROM）または CRS モデルに依存している。しかし、信頼されたセットアップモデル（すなわち通常モデル外）において、もし中央集権的存在がバックドアを仕込んだ場合、その NIBS の安全性はもはや保証されない。実際、[6] では、通常モデルにおける NIBS の構成が可能であるかどうかについて、未解決問題としている。より最近では、[10] が通常モデルにおける初の NIBS を構成した。しかし、この NIBS は Complexity Leveraging に依存しており、より大きなパラメータを必要とし、効率を著しく低下させる。さらに、この NIBS は *Weak blindness* しか満たさず、*Strong blindness* を満たす通常モデルの構成は依然として未解決問題として残されている。

これらの結果は自然に次の問いへと導かれる：ROM や CRS に依存せず、標準的な仮定の下で Strong Blindness を達成する NIBS を構築できるだろうか？

本研究の貢献は、この問いに対して否定的な結果を与えることである。我々は、攻撃者をブラックボックス的に利用する限り、そのような NIBS の構築は困難であることを示す。具体的には、統計的に Strong Blindness を満たす NIBS の偽造不能性を非対話型の仮定に帰着させる単純帰着が存在しないことを示す。

2. 前提知識

セキュリティパラメータを $\lambda \in \mathbb{Z}$ とする。すべてのアルゴリズムは、入力として暗黙的に λ を受け取るものとする。最初の N 個の自然数を $[N] := 1, \cdots, N$ と表記する。有限集合 S に対して、$x \leftarrow S$ は x が S から一様ランダムにサンプリングされることを意味する。確率的アルゴリズム $\mathcal{A}$ に対して、$y \leftarrow \mathcal{A}(x)$ は、入力 x に対して $\mathcal{A}$ が一様にサンプリングされた乱数を用いて出力する値 y を意味する。初期化乱数 ρ を明示する場合、$y \leftarrow \mathcal{A}(x; \rho)$ と書く。また、$y \in \mathcal{A}(x)$ は y が $\mathcal{A}(x)$ の出力の一つであることを意味する。さらに、$\mathcal{A}^{\mathcal{O}}(x)$ は、$\mathcal{A}$ がオラクル $\mathcal{O}$ にアクセス可能であることを表す。

関数 $f : \mathbb{N} \to \mathbb{R}_+$ が入力 n に関して無視可能（negligible）であるとは、$f(n) = \mathsf{negl}(n)$ すなわち $f \in n^{-\omega(1)}$ であることをいう。

アルゴリズムが確率的多項式時間（probabilistic polynomial time, PPT）であるとは、その実行時間が入力サイズに対する多項式で上界付けられる場合をいう。さらに、$\mathsf{poly}(n)$ を n の多項式全体の集合とし、$k = \mathsf{poly}(n)$ は $k \in \mathsf{poly}(n)$ を意味する。

2.1 非対話型仮定

定義 1 (困難な非対話型仮定)**.** 非対話型（暗号的）問題 $P = (I, V)$ は、次の二つの *PPT* アルゴリズムから構成される：

インスタンス生成 $I(\lambda) \to y$**:** セキュリティパラメータ λ を入力として、インスタンス y を出力する。

インスタンス検証 $V(x, y) \to b$**:** 解 x とインスタンス y を

入力として、ビット $b \in \{0,1\}$ を出力する。

P が困難な非対話型問題であるとは、次の性質を満たす場合をいう：

困難性　あらゆる PPT 攻撃者 $\mathcal{A}$ に対して、以下の確率は無視可能である：

$$\Pr\left[V(x', y) = 1, |, y \leftarrow I(\lambda); , x' \leftarrow \mathcal{A}(y)\right].$$

例えば、関数 f が一方向関数であるという仮定は困難な非対話仮定であり、1 ラウンドのゲームとしてモデル化できる。このゲームでは、チャレンジャーが一様ランダムな x に対して $y = f(x)$ を攻撃者 $\mathcal{A}$ に送信し、$\mathcal{A}$ が $f(x') = y$ を満たす x' を返すことに成功すれば（すなわちゲームが Accept 出力すれば）、勝利とみなされる。

2.2　ブラックボックス帰着

次に、本研究で議論するブラックボックス帰着の概念を説明する。我々の定式化は主に [12] に従う。具体的には、二つの仮定 C_1 と C_2 が与えられたとき、C_1 の困難性を C_2 の困難性にブラックボックス的に基づけるとは、C_2 を破る攻撃者 $\mathcal{A}_2$ が与えられたときに、その $\mathcal{A}_2$ をオラクルとして用いて C_1 を破る多項式時間で動く帰着 $\mathcal{R}$ が構成できることを意味する。

特筆すべき点として、$\mathcal{R}$ が $\mathcal{A}_2$ を 1 回だけ呼び出す必要はなく、多項式回数呼び出すことができ、これらの呼び出しは入れ子になっていてもよい。この文脈において、$\mathcal{A}_2$ は（場合によっては非一様な）攻撃者とみなされ、$\mathcal{R}$ は $\mathcal{A}_2$ へのオラクルアクセスを持つ多項式時間帰着となる。

定義 2 (ブラックボックス帰着)**.** 確率的多項式時間アルゴリズム $\mathcal{R}$ が、仮定 C_1 から仮定 C_2 へのブラックボックス帰着であるとは、任意の C_1 を破る決定論的攻撃者 $\mathcal{A}$ に対して、帰着 $\mathcal{R}^{\mathcal{A}}$ が C_2 を破る場合をいう。

本研究では、帰着 $\mathcal{R}$ がアクセスする攻撃者 $\mathcal{A}$ を決定論的（あるいは固定された乱数を持つ）に制限する。この制約により、帰着は必要に応じて攻撃者を巻き戻したり、再起動したりすることが可能となる。

さらに、 [11], [12] に従い、固定パラメータ帰着に焦点を当てる。ここでは、帰着は単一のセキュリティパラメータに対して攻撃者を呼び出すことが許される。すなわち、セキュリティパラメータ λ に対して、帰着はパラメータ化された攻撃者 $\mathcal{A}(1^\lambda)$ の $M(\lambda)$ インスタンスまで実行でき、すべての呼び出しで同じ攻撃者を用いなければならない。

2.3　非対話ブラインド署名 (Non-Interactive Blind Signature)

次に、非対話ブラインド署名（NIBS）を定義する。ここでは、署名者の公開乱数を nonce とみなす簡略化された Syntax を [1] に従って採用する。

定義 3 (非対話ブラインド署名 (NIBS))**.** 非対話型盲署名スキーム $\mathsf{NIBS} = (\mathsf{KeyGen}, \mathsf{RKeyGen}, \mathsf{Issue}, \mathsf{Obtain}, \mathsf{Verify})$ は、以下の PPT アルゴリズムから構成される：

$\mathsf{KeyGen}(\lambda) \to (\mathsf{sk}, \mathsf{pk})$**:** セキュリティパラメータ λ を入力として、署名者の鍵ペア $(\mathsf{sk}, \mathsf{pk})$ を出力する。ここで、pk は暗黙的にノンス空間 $\mathcal{N}_{\mathsf{pk}}$ を定義する。

$\mathsf{RKeyGen}(\lambda) \to (\mathsf{rsk}, \mathsf{rpk})$**:** セキュリティパラメータ λ を入力として、受信者の鍵ペア $(\mathsf{rsk}, \mathsf{rpk})$ を出力する。

$\mathsf{Issue}(\mathsf{sk}, \mathsf{rpk}) \to (\mathsf{psig}, \mathsf{nonce})$**:** 署名者の秘密鍵 sk と受信者の公開鍵 rpk を入力として、事前署名 psig とノンス nonce を出力する。ここで、ノンスは署名者の公開乱数の一部を表す。

$\mathsf{Obtain}(\mathsf{rsk}, \mathsf{pk}, (\mathsf{psig}, \mathsf{nonce})) \to (\mathsf{m}, \mathsf{sig})$**:** 受信者の秘密鍵 rsk、署名者の公開鍵 pk、および事前署名 - ノンスのペア $(\mathsf{psig}, \mathsf{nonce})$ を入力として、有効なメッセージ - 署名ペア $(\mathsf{m}, \mathsf{sig})$ あるいは $\perp$ を出力する。

$\mathsf{Verify}(\mathsf{pk}, \mathsf{m}, \mathsf{sig}) \to b$**:** 署名者の公開鍵 pk とメッセージ - 署名ペア $(\mathsf{m}, \mathsf{sig})$ を入力として、その署名が有効であるかを示すビット $b \in \{0,1\}$ を出力する。

NIBS は 正当性 *(correctness)*、再利用可能性 *(reusability)*、偽造不能性、および *strong blindness* を満たすことを要求する。（紙面の都合上、各優位性の正確な定義は本論文では省略する。詳しくは [1] を参照すること）

定義 4 (正当性 (Correctness))**.** NIBS スキームは、すべての $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(\lambda)$ および $(\mathsf{rsk}, \mathsf{rpk}) \leftarrow \mathsf{RKeyGen}(\lambda)$ に対して署名生成と検証が可能であるとき、正当性を有すると言う。

再利用性 *(Reusability)* は [1] によって初めて導入され、異なるノンスの下で生成された事前署名から、受信者が 2 つの異なるメッセージと有効な署名を得られることを保証する。

定義 5 (再利用性 (Reusability))**.** NIBS が任意の λ に対して署名者が正当に複数の事前署名を発行した際にメッセージが重複しない場合、再利用性 *(Reusability)* を満たすという。

我々の 偽造不能性 の定義は、構文を [1] に従っているため、[6] ではなく [1] に基づく。

定義 6 (偽造不可能性)**.** NIBS スキームは、任意の PPT 攻撃者 $\mathcal{A}$ に対して次の優位性が λ において無視可能であるとき、偽造不可能性を満たすという：

$$\mathbf{Adv}^{\ell\text{-OMUF}}_{\mathsf{NIBS},\mathcal{A}}(\lambda) := \Pr\left[\ell\text{-}\mathsf{OMUF}^{\mathcal{A}}_{\mathsf{NIBS}}(\lambda) = 1\right],$$

Strong blindness は、[6] で定義された blindness の強化版であり、[1] によって改良され、複数の事前署名が関与する状況においてより強固なプライバシ保証を与える。

定義 7 (Strong Recipient Blindness)**.** NIBS は、すべての PPT（それぞれ非制限）攻撃者 $\mathcal{A}$ に対して次の優位性が λ において無視可能であるとき, *Strong recipient blindness* を満たすという：

$$\mathbf{Adv}^{q\text{-rbnd}}_{\mathsf{NIBS},\mathcal{A}}(\lambda) := 2\Pr\left[q\text{-}\mathsf{RBND}^{\mathcal{A}}_{\mathsf{NIBS}}(\lambda)=1\right]-1,$$

定義 8 (Strong Nonce Blindness)**.** NIBS は、すべての *PPT* 攻撃者 $\mathcal{A}$ に対して次の優位性が λ において無視可能であるとき、*Strong Blindness* を満たすという：

$$\mathbf{Adv}^{q\text{-nbnd}}_{\mathsf{NIBS},\mathcal{A}}(\lambda) := 2\Pr\left[q\text{-}\mathsf{NBND}^{\mathcal{A}}_{\mathsf{NIBS}}(\lambda)=1\right]-1,$$

3. 統計的 blindness を満たす NIBS の構成不可能性

一般の帰着に対する不可能性証明を与える前に、より単純なクラスの帰着を考察する。我々はこれを単純帰着 *(simple reductions)* と呼ぶ。

定義 9 (単純帰着)**.** 固定パラメータを持つブラックボックス帰着 $\mathcal{R}$ が次を満たすとき、単純帰着であるという：

- $\mathcal{R}$ は攻撃者の実行を *1* 回のみ行う。
- $\mathcal{R}$ は攻撃者を巻き戻さない。

3.0.1 汎用偽造オラクル

「理想的」攻撃者を定義するために、まず汎用偽造オラクル を導入する。これは理想的攻撃者の無限の計算能力に基づく手続きを抽象化したものである。

直感的には、汎用偽造オラクル Σ は署名者の公開鍵、受信者の公開鍵、事前署名 - ノンスのペアを入力とし、与えられたデータから導出されうるメッセージ - 署名ペアを総当たりで求め、その一つをランダムに返す:

定義 10 (汎用偽造オラクル)**.** 汎用偽造オラクル $\Sigma(\mathsf{pk},\mathsf{rpk},(\mathsf{psig},\mathsf{nonce}))$ は以下のように動作する：

(1) $(\mathsf{rsk}',\mathsf{rpk}) \in \mathsf{RKeyGen}(\lambda)$ を満たすすべての受信者秘密鍵 rsk' と、アルゴリズム $\mathsf{Obtain}(\mathsf{rsk}',\mathsf{pk},(\mathsf{psig},\mathsf{nonce});r')$ のすべての乱数 r' を列挙し、有効なメッセージ - 署名ペアを生成できるものを記録する。

(2) 集合から (rsk',r') をランダムに選択（存在しなければ $\perp$ を返す）、次に有効なメッセージ - 署名ペア $(\mathsf{m},\mathsf{sig}) \leftarrow \mathsf{Obtain}(\mathsf{rsk}',\mathsf{pk},(\mathsf{psig},\mathsf{nonce});r')$ を返す。

乱数 s を明示する場合は $\Sigma(\mathsf{pk},\mathsf{rpk},(\mathsf{psig},\mathsf{nonce});s)$ と書き、rsk' と r' が s によって決定的に選ばれることを意味する。

3.0.2 理想的攻撃者

次に、NIBS の 偽造不能性を破るために無限の計算力を持つ**理想的攻撃者**を定義する。

直感的には、理想的攻撃者 $\mathcal{A}^{\Sigma}$ は 偽造不能性ゲームを通じて 1 つのメッセージ - 署名ペアを獲得し、汎用偽造オラクルを用いて 2 つ目のペアを生成する（当然、無限の計算力を持つため Σ を内部的にシミュレートできる）。

定義 11 (理想的攻撃者)**.** NIBS を *NIBS* とする。 偽造不能性に対する理想的攻撃者 $\mathcal{A}^{\Sigma}$ は以下の手順で動作する：

(1) 偽造不能性ゲームから公開鍵 pk を受け取ったら、受信者鍵ペア $(\mathsf{rsk},\mathsf{rpk}) \leftarrow \mathsf{RKeyGen}(\lambda)$ をサンプリングする。

(2) rpk をゲームに送信し、事前署名 - ノンスのペア $(\mathsf{psig},\mathsf{nonce})$ を受け取る。

(3) $(\mathsf{m},\mathsf{sig}) \leftarrow \mathsf{Obtain}(\mathsf{rsk},\mathsf{pk},(\mathsf{psig},\mathsf{nonce}))$ を計算する。

(4) もし $\mathsf{Verify}(\mathsf{pk},\mathsf{m},\mathsf{sig})=1$ なら、*2* つ目の偽造を計算する：

$$(\mathsf{m}',\mathsf{sig}') \leftarrow \Sigma(\mathsf{pk},\mathsf{rpk},(\mathsf{psig},\mathsf{nonce})).$$

そうでなければ $(\mathsf{m},\mathsf{sig})$ および $(\mathsf{m}',\mathsf{sig}')$ を $\perp$ に設定する。

(5) $(\mathsf{m},\mathsf{sig})$ と $(\mathsf{m}',\mathsf{sig}')$ を偽造として出力する。

一見すると、理想的攻撃者は勝利できないように思える。なぜなら 偽造不能性ゲームで得たメッセージと、汎用偽造オラクルが生成するメッセージが一致する可能性があるからである（すなわち $\mathsf{m}=\mathsf{m}'$）。しかし、補題 1 は、NIBS が統計的 blindness と再利用性を満たす限り、この事象は無視可能な確率でしか起こらないことを保証する。したがって理想的攻撃者は圧倒的確率で成功する。紙面の都合上、証明は省く。

補題 1. 理想的攻撃者 $\mathcal{A}^{\Sigma}$ は偽造不能性ゲームにおいて、無視可能な確率を除いて勝利する。すなわち、

$$\Pr\left[1\text{-}\mathsf{OMUF}^{\mathcal{A}^{\Sigma}}_{\mathsf{NIBS}}(\lambda)=1\right] = 1-\mathsf{negl}(\lambda).$$

3.1 秘密鍵独立性

ここで、統計的 recipient blindness よりも弱いが、本稿後半で示すメタ帰着シミュレーションと理想的攻撃者の振る舞いの区別不可能性を示す上で本質的な概念である**秘密鍵独立性**を導入する。

直感的には、秘密鍵独立性ゲームにおいて、悪意ある署名者は、独立した秘密鍵を用いて生成された 2 つのメッセージ - 署名対が、同一の事前署名 - ノンス対から導かれたものか、それとも異なるペアから導かれたものかを区別しようとする。重要な点として、統計的 blindness を持つ NIBS における各公開鍵が複数の有効な秘密鍵に対応する場合があるという点である:

定義 12 (秘密鍵独立性)**.** 任意の攻撃者 $\mathcal{A}$ に対して、次の優位性が λ において無視可能であるとき、NIBS は秘密鍵独立性を満たすという：

$$\mathbf{Adv}^{\mathsf{skind}}_{\mathsf{NIBS},\mathcal{A}}(\lambda) := 2\Pr\left[\mathsf{SKINDNIBS}^{\mathcal{A}}(\lambda)=1\right]-1,$$

次に、すべての NIBS が秘密鍵独立性を満たすことを示す。

補題 2. もし NIBS が統計的 *recipient blindness* を満たすならば、それは秘密鍵独立性も満たす。

証明. NIBS の秘密鍵独立性に対する攻撃者 $\mathcal{A}$ を仮定する。我々はこれを利用して統計的 recipient blindness に対

抗する PPT アルゴリズム $\mathcal{R}$ を構成する。帰着 $\mathcal{R}$ は次のように動作する：

(1) ゲームから受信者公開鍵 $(\mathsf{rpk}_0, \mathsf{rpk}_1)$ を受け取ったら、

$$(\mathsf{pk}, \mathsf{psig}_0, \mathsf{nonce}_0, \mathsf{psig}_1, \mathsf{nonce}_1) \leftarrow \mathcal{A}(\mathsf{rpk}_0, \mathsf{rpk}_1),$$

を計算し、このタプルをゲームに渡す。

(2) ゲームからチャレンジ $(\mathsf{m}_b, \mathsf{sig}_b, \mathsf{m}_{1-b}, \mathsf{sig}_{1-b})$ を受け取ったら、次を計算する：

$$(\mathsf{m}', \mathsf{sig}') \leftarrow \Sigma(\mathsf{pk}, \mathsf{rpk}_1, (\mathsf{psig}_1, \mathsf{nonce}_1)).$$

（もし $(\mathsf{m}_b, \mathsf{sig}_b) = \perp$ なら $(\mathsf{m}', \mathsf{sig}') := \perp$ とする。）

(3) $\mathcal{R}$ は

$$b' \leftarrow \mathcal{A}(\mathsf{m}_b, \mathsf{sig}_b, \mathsf{m}', \mathsf{sig}'),$$

を実行し、最終的に b' をゲームに返す。

$b = 0$ の場合は $\mathcal{A}$ が秘密鍵独立性ゲームで受け取る入力と一致し、$b = 1$ の場合も同様に一致する。したがって、$\mathcal{R}$ の recipient blindness ゲームにおける優位性は $\mathcal{A}$ の秘密鍵独立性ゲームにおける優位性と一致する。前者が無視可能である以上、後者も無視可能である。 □

NIBS の安全性を非対話型仮定に帰着させる単純帰着は存在しないことを示す。

定理 1. NIBS が非対話型かつ統計的 *blindness* を満たす署名であるとする。このとき、NIBS の偽造不可能性から困難な非対話型仮定への単純帰着は存在しない。

証明. $\mathcal{R}$ を単純帰着とする。$\mathcal{R}$ は困難な非対話型問題のインスタンス y を入力として受け取り、（リセット不可能かつブラックボックスな）偽造不可能性に対する攻撃者 $\mathcal{A}$ へのオラクルアクセスを持つ。$\mathcal{R}$ の目的は、y の解を出力することである。

メタ帰着 $\mathcal{M}$ は、困難な問題インスタンス y を入力として以下のように動作する。

(1) $\mathcal{M}$ は固定された乱数 $r_{\mathcal{R}}$ を用いて単純帰着 $\mathcal{R}$ を y の入力で実行し、署名者の公開鍵 pk（および攻撃者の初期乱数）を得る。

(2) $(\mathsf{rsk}, \mathsf{rpk}) \leftarrow \mathsf{RKeyGen}(\lambda)$ をサンプリングし、rpk を $\mathcal{R}$ に送って、署名前署名–ナンス対 $(\mathsf{psig}, \mathsf{nonce})$ を受け取る。

(3) $\mathcal{M}$ は $(\mathsf{m}, \mathsf{sig}) \leftarrow \mathsf{Obtain}(\mathsf{rsk}, \mathsf{pk}, (\mathsf{psig}, \mathsf{nonce}))$ を計算する。次に、二つ目の有効なメッセージ–署名対を得るために、新たなコピー $\mathcal{R}'$ を同じ入力 y と乱数 $r_{\mathcal{R}}$ で実行し、同じ pk を生成させる。

(4) $(\mathsf{rsk}', \mathsf{rpk}') \leftarrow \mathsf{RKeyGen}(\lambda)$ をサンプリングし、rpk' を $\mathcal{R}'$ に送って $(\mathsf{psig}', \mathsf{nonce}')$ を得る。

(5) $(\mathsf{m}', \mathsf{sig}') \leftarrow \mathsf{Obtain}(\mathsf{rsk}', \mathsf{pk}, (\mathsf{psig}', \mathsf{nonce}'))$ を計算し、$\mathcal{R}'$ を中止して、$(\mathsf{m}, \mathsf{sig})$ および $(\mathsf{m}', \mathsf{sig}')$ を $\mathcal{R}$ に渡して出力 x' を得る。最後に、$\mathcal{M}$ は x' を出力する。

ここで、単純帰着 $\mathcal{R}$ が非自明な確率で y の解を出力することを示す。$\mathcal{R}^{\mathcal{A}^\Sigma}$ を理想的攻撃者 $\mathcal{A}^\Sigma$ と対話実行する場合の帰着、$\mathcal{R}^{\mathcal{M}}$ をメタ帰着 $\mathcal{M}$ と対話実行する場合の帰着とする。

$\mathcal{A}^\Sigma$ は 2 つの有効なメッセージ–署名対を成功裏に出力する（補題 1）。したがって、$\mathcal{R}^{\mathcal{A}^\Sigma}$ と $\mathcal{R}^{\mathcal{M}}$ の成功確率がほぼ同等であることを示せば十分である。

このために、秘密鍵独立性ゲームからの帰着 $\mathcal{R}^*$ を以下のように定義する。

(1) $\mathcal{R}^*$ はゲームから受信者公開鍵 $\mathsf{rpk}_0, \mathsf{rpk1}$ を受け取る。

(2) $y \leftarrow I(\lambda)$ をサンプリングし、$\mathcal{R}(y; r\mathcal{R})$ を実行して pk を得る。

(3) rpk_0 を $\mathcal{R}$ に送り、$(\mathsf{psig}, \mathsf{nonce})$ を得る。

(4) 同じ入力と乱数で $\mathcal{R}'$ を実行し、rpk_1 を使って $(\mathsf{psig}', \mathsf{nonce}')$ を得る。

(5) $\mathcal{R}'$ を中止し、$(\mathsf{pk}, \mathsf{psig}', \mathsf{nonce}', \mathsf{psig}, \mathsf{nonce})$ をゲームに送信する。

(6) ゲームから $(\mathsf{m}b, \mathsf{sig}b, \mathsf{m1}-b, \mathsf{sig1}-b)$ を受け取り、それを $\mathcal{R}$ に渡して x' を得る。最後に $b' \leftarrow V(x', y)$ を返す。

ここで、$b = 0$ の場合はシミュレーションが $\mathcal{M}$ と一致し、$b = 1$ の場合は $\mathcal{A}^\Sigma$ をシミュレートする。Z に対して $x' \leftarrow \mathcal{R}^Z(y)$、$y \leftarrow I(\lambda)$ のとき、$V(x', y) = 1$ である事象を $\mathsf{Succ}(Z)$ とすると：

$$\begin{aligned}
&\Pr[\mathsf{Succ}(\mathcal{A}^\Sigma)] - \Pr[\mathsf{Succ}(\mathcal{M})] \\
&\quad = \Pr[b' = 1 \mid b = 1] - \Pr[b' = 1 \mid b = 0] \\
&\quad = \mathbf{Adv}^{\mathsf{skind}}_{\mathsf{NIBS}, \mathcal{R}^*}(\lambda).
\end{aligned}$$

補題 2 により、統計的 recipient blindness は秘密鍵独立性を含意するため、

$$\Pr[\mathsf{Succ}(\mathcal{M})] = \Pr[\mathsf{Succ}(\mathcal{A}^\Sigma)] + \mathsf{negl}(\lambda).$$

が成り立つ。さらに、補題 1 から

$$\Pr[\mathsf{Succ}(\mathcal{A}^\Sigma)] = 1 - \mathsf{negl}(\lambda),$$

が得られる。なぜなら、

$$\Pr\left[\text{1-OMUF}^{\mathcal{A}^\Sigma}_{\mathsf{NIBS}}(\lambda) = 1\right] = \Pr[\mathsf{Succ}(\mathcal{A}^\Sigma)],$$

が、$\mathcal{R}$ が単純帰着であるという仮定の下で成立するからである。したがって、$\Pr[\mathsf{Succ}(\mathcal{M})]$ も $1 - \mathsf{negl}(\lambda)$ となり、これは y を解くことが困難であるという仮定と矛盾する。 □

4. 計算量的 blindness を満たす NIBS の構成不可能性

我々は統計的 blindness に対する不可能性結果を、計算的 blindness へと拡張する。

4.0.1 汎用偽造オラクル

まず、計算的設定に合わせた汎用偽造オラクルの変種を導入する。統計的設定で用いた汎用偽造オラクルはそのままでは適用できない。というのも、計算的 blindness は単一のトランスクリプトから複数のメッセージ - 署名対を導出できることを必ずしも保証しないためである。その帰結として、統計的設定のために構成した理想的攻撃者は、計算的設定では偽造不能性ゲームに勝てない場合がある。

直感的には、計算的設定における我々の汎用偽造オラクルは、署名者の公開鍵 pk を入力として受け取り、無限計算力を用いて対応する秘密鍵 sk を回収する。続いて、有効な事前署名 - ノンス対を生成し、最終的に有効なメッセージ - 署名対を生成する。これにより、計算的 blindness のみを仮定する状況でも偽造のシミュレーションが可能になる。

定義 13 (汎用偽造オラクル)**.** NIBS を非対話ブラインド署名とする。汎用偽造オラクル $\Sigma_c(\mathsf{pk}, \mathsf{rpk})$ は次のように動作する*:*

(1) $(\mathsf{sk}', \mathsf{pk}) \in \mathsf{Gen}(\lambda)$ を満たすすべての秘密鍵 sk' を列挙してリストに保存する（そのような sk' が存在しなければ $\perp$ を出力)。

(2) 保存したリストからランダムに鍵 sk' を選び，$(\mathsf{psig}, \mathsf{nonce}) \leftarrow \mathsf{Issue}(\mathsf{sk}', \mathsf{pk})$ を計算する*.*

(3) ペア $(\mathsf{psig}, \mathsf{nonce})$ を返す。

乱数 s を明示する場合は $\Sigma_c(\mathsf{pk}, \mathsf{rpk}; s)$ と書く。

4.0.2 理想的攻撃者

汎用偽造オラクル Σ_c を用いて、計算的設定に適合した理想的攻撃者 $\mathcal{A}^{\Sigma_c}$ を構成できる。

定義 14 (理想的攻撃者)**.** NIBS を非対話ブラインド署名とする。偽造不能性に対する理想的攻撃者 $\mathcal{A}^{\Sigma_c}$ は次のように動作する*:*

(1) 偽造不能性ゲームから公開鍵 pk を受け取る。

(2) 受信者鍵ペア $(\mathsf{rsk}, \mathsf{rpk}) \leftarrow \mathsf{RKeyGen}(\lambda)$ を生成し，rpk をゲームに送る。

(3) 事前署名 - ノンス対 $(\mathsf{psig}, \mathsf{nonce})$ を受け取る

- もし $\mathsf{Verify}(\mathsf{pk}, \mathsf{m}, \mathsf{sig}) = 1$ なら，新たな受信者鍵ペア $(\mathsf{rsk}', \mathsf{rpk}') \leftarrow \mathsf{RKeyGen}(\lambda)$ を生成し，
- そうでなければ $(\mathsf{m}, \mathsf{sig}) :=\perp$ および $(\mathsf{m}', \mathsf{sig}') :=\perp$ とする。

(4) $(\mathsf{m}, \mathsf{sig}, \mathsf{m}', \mathsf{sig}')$ を偽造として出力する。

理想的な攻撃者 $\mathcal{A}^{\Sigma_c}$ が 偽造不能性ゲームに成功することを示す前に、汎用偽造オラクル Σ_c に相対化された新しい blindness の性質を導入する。この概念は計算的設定における秘密鍵独立性も意味し、その定義は後に与える。

定義 15 (汎用偽造オラクルに対する blindness)**.** $\mathsf{NIBS} = (\mathsf{KeyGen}, \mathsf{RKeyGen}, \mathsf{Issue}, \mathsf{Obtain}, \mathsf{Verify})$ を非対話型ブラインド署名とする。NIBS が汎用偽造オラクル Σ_c に対する計算的 *blindness* を満たすとは、適応的に Σ_c へアクセス可能な任意の *PPT* アルゴリズム $\mathcal{A}^{\Sigma_c}$ に対して、以下の両方の優位性が λ において無視可能であることをいう：

次の補題は、理想的な攻撃者 $\mathcal{A}^{\Sigma_c}$ が高い確率で 偽造不能性ゲームに勝利することを主張する。

補題 3. NIBS が汎用偽造オラクル Σ_c に対する *blindness* を満たすとする。このとき、理想的な攻撃者 $\mathcal{A}^{\Sigma_c}$ は NIBS の 偽造不能性ゲームに無視できる確率を除いて勝利する。

証明. $\mathsf{m} \neq \mathsf{m}'$ が高い確率で成り立つことを示せば十分である。

この証明は補題 1 と同様のアイデアに従うが、ここではナンス blindness の代わりに受信者 blindness を用いる。我々は受信者 blindness に対する攻撃者 $\mathcal{A}^{\Sigma_c}$ を次のように定義する：

(1) $\mathcal{A}^{\Sigma_c}$ は誠実に署名者鍵ペア $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(\lambda)$ を生成する。その後次を計算する：

$$(\mathsf{psig}_0, \mathsf{nonce}_0) \leftarrow \mathsf{Issue}(\mathsf{sk}, \mathsf{rpk}_0), \quad (\mathsf{psig}_1, \mathsf{nonce}_1) \leftarrow \mathsf{Issue}(\mathsf{sk}, \mathsf{rpk}$$

そして両方をゲームに送信する。

(2) チャレンジのメッセージ・署名対 $(\mathsf{m}_b, \mathsf{sig}_b, \mathsf{m}_{1-b}, \mathsf{sig}_{1-b})$ を受け取った後、次を計算する：

$$(\mathsf{m}', \mathsf{sig}') \leftarrow \mathsf{Obtain}(\mathsf{rsk}_1, \mathsf{pk}, \Sigma_c(\mathsf{pk}, \mathsf{rpk}_1)).$$

(3) もし $\mathsf{m}_b \neq \mathsf{m}'$ なら $b' = 0$ を、そうでなければ $b' = 1$ を出力する。

$p = \Pr[\mathsf{m}_1 = \mathsf{m}']$ とする。これは $\mathcal{A}^{\Sigma_c}$ が 偽造可能性ゲームに敗北する確率である。正当性より $(\mathsf{m}_1, \mathsf{sig}_1) \neq \perp$ が成り立ち、再利用性より $\mathsf{m}_0 \neq \mathsf{m}_1$ が成り立つ（無視可能な確率を除く)。したがって次を得る：

$$\Pr[b = b'] = \Pr[b = b' \mid \mathsf{m}_0 \neq \mathsf{m}_1] + \mathsf{negl}(\lambda).$$

次を解析する：- $b = 0$ かつ $\mathsf{m}_1 = \mathsf{m}'$ のとき、$\mathsf{m}_0 \neq \mathsf{m}'$ なので $b' = 0$。- $b = 1$ かつ $\mathsf{m}_1 = \mathsf{m}'$ のとき、$b' = 1$。

したがって：

$$\Pr[b = b', \mathsf{m}_1 = \mathsf{m}' \mid \mathsf{m}_0 \neq \mathsf{m}_1] = \frac{p}{2}.$$

一方で：- $b = 0$ かつ $\mathsf{m}_1 \neq \mathsf{m}'$ のとき、$b' = 0$（勝利)。- $b = 1$ かつ $\mathsf{m}_1 \neq \mathsf{m}'$ のとき、$b' = 0$（敗北)。

よって：

$$\Pr[b = b', \mathsf{m}_1 \neq \mathsf{m}' \mid \mathsf{m}_0 \neq \mathsf{m}_1] = \frac{1}{2} + \mathsf{negl}(\lambda).$$

両者を足し合わせると：

$$\Pr[b = b' \mid \mathsf{m}_0 \neq \mathsf{m}_1] = \frac{p+1}{2} + \mathsf{negl}(\lambda).$$

したがって：

$$\mathbf{Adv}^{\mathsf{rbnd}}_{\mathsf{NIBS},\mathcal{A}}(\lambda) = p + \mathsf{negl}(\lambda),$$

これにより、受信者 blindness の仮定から p は無視可能で

あることが導かれる。 □

次に、計算的設定に適した **計算的秘密鍵独立性** の概念を導入する。この概念は、与えられたメッセージ-署名対が正直な署名者によって生成されたものか、あるいは汎用偽造オラクルから得られたものかを区別できないことを捉える。定義は統計的な場合と対応しており、計算的考慮に必要な調整を加えたものである。

定義 16 (計算的秘密鍵独立性)**.** NIBS が 計算的秘密鍵独立性 を満たすとは、任意の PPT 攻撃者 $\mathcal{A}$ に対して、次の優位性が λ において無視可能であることをいう：

$$\mathbf{Adv}^{\mathsf{cskind}}_{\mathsf{NIBS},\mathcal{A}}(\lambda) := 2\Pr\left[\mathsf{cSKIND}^{\mathcal{A}}_{\mathsf{NIBS}}(\lambda)=1\right]-1.$$

統計的な場合と同様に、汎用偽造オラクルに対する計算的受領者 blindness を満たす任意の NIBS は、計算的秘密鍵独立性も満たすことを示すことができる。

補題 4. NIBS が汎用偽造オラクル Σ_c に対する計算的受領者 *blindness* を満たすならば、それはまた計算的秘密鍵独立性も満たす。

証明. $\mathcal{A}$ を計算的秘密鍵独立性に対する PPT 攻撃者とする。我々は、汎用偽造オラクル Σ_c へのアクセスを持つ受信者 blindness ゲームに対する PPT 攻撃者 $\mathcal{R}^{\Sigma_c}$ を次のように構成する：

(1) blindness ゲームから受信者公開鍵 rpk' を受け取ったら、新しい受信者鍵ペア $(\mathsf{rsk},\mathsf{rpk}) \leftarrow \mathsf{RKeyGen}(\lambda)$ を生成する。

(2) $(\mathsf{rpk},\mathsf{rpk}')$ を入力として $\mathcal{A}$ を実行し、次を得る：

$$(\mathsf{pk},\mathsf{psig},\mathsf{nonce},\mathsf{psig}',\mathsf{nonce}') \leftarrow \mathcal{A}(\mathsf{rpk},\mathsf{rpk}').$$

(3) メッセージ・署名対を計算する：

$$(\mathsf{m},\mathsf{sig}) \leftarrow \mathsf{Obtain}(\mathsf{rsk},\mathsf{pk},(\mathsf{psig},\mathsf{nonce})).$$

(4) 汎用偽造オラクルを用いて新たな事前署名・ナンス対を取得する：

$$(\mathsf{psig}_1,\mathsf{nonce}_1) \leftarrow \Sigma_c(\mathsf{pk},\mathsf{rpk}').$$

(5) $(\mathsf{psig}',\mathsf{nonce}',\mathsf{psig}_1,\mathsf{nonce}_1)$ をゲームに送信し、メッセージ・署名対 $(\mathsf{m}_b,\mathsf{sig}_b)$ および $(\mathsf{m}_{1-b},\mathsf{sig}_{1-b})$ を受け取る。

(6) もし $(\mathsf{m}_b,\mathsf{sig}_b) = \perp$ なら、$(\mathsf{m},\mathsf{sig}) := \perp$ とする。

(7) 次を実行する：

$$b' \leftarrow \mathcal{A}(\mathsf{m},\mathsf{sig},\mathsf{m}_b,\mathsf{sig}_b),$$

そして b' をゲームに出力する。

$\mathcal{R}^{\Sigma_c}$ のシミュレーションが秘密鍵独立性ゲームに対応していることを示す：

- blindness ゲームにおいて $b=0$ の場合、ゲームは $(\mathsf{m}_0,\mathsf{sig}_0)$ と $(\mathsf{m}_1,\mathsf{sig}_1)$ をその順で返す。このとき $\mathcal{R}^{\Sigma_c}$ は $(\mathsf{m},\mathsf{sig},\mathsf{m}_0,\mathsf{sig}_0)$ を $\mathcal{A}$ に渡す。これは cSKIND ゲームの $b=0$ の分岐に一致する。
- $b=1$ の場合、ゲームは順序を入れ替えて $(\mathsf{m}_1,\mathsf{sig}_1)$ と $(\mathsf{m}_0,\mathsf{sig}_0)$ を返す。このとき $\mathcal{R}^{\Sigma_c}$ は $(\mathsf{m},\mathsf{sig},\mathsf{m}_1,\mathsf{sig}_1)$ を $\mathcal{A}$ に渡し、これは cSKIND ゲームの $b=1$ の場合に一致する。

したがって、$\mathcal{R}^{\Sigma_c}$ は秘密鍵独立性ゲームを完全にシミュレートする。よって、秘密鍵独立性に対する $\mathcal{A}$ の利得は、受信者 blindness に対する $\mathcal{R}^{\Sigma_c}$ の利得によって上界され、仮定よりこれは無視可能である。

□

定理 2. NIBS が汎用偽造オラクルに対して計算的 *blindness* を満たす非対話型ブラインド署名方式であるとする。このとき、NIBS の 偽造不能性から困難な非対話型仮定への単純なブラックボックス帰着は存在しない。

証明. $\mathcal{R}$ を、困難な非対話型問題インスタンス y を入力とし、 偽造不能性ゲームに対する攻撃者 $\mathcal{A}$ へのブラックボックスアクセスを持つ単純帰着とする。$\mathcal{R}$ は最終的に y の解候補を出力する。

攻撃者をシミュレートするメタ帰着 $\mathcal{M}$ を構成する。問題インスタンス y を入力としたとき、$\mathcal{M}$ は次のように動作する：

(1) 固定した乱数 $r_{\mathcal{R}}$ を用いて $\mathcal{R}(y;r_{\mathcal{R}})$ を実行し、署名者の公開鍵 pk を得る。

(2) $(\mathsf{rsk},\mathsf{rpk}) \leftarrow \mathsf{RKeyGen}(\lambda)$ を生成し、rpk を $\mathcal{R}$ に渡し、$(\mathsf{psig},\mathsf{nonce})$ を受け取る。

(3) $(\mathsf{m},\mathsf{sig}) \leftarrow \mathsf{Obtain}(\mathsf{rsk},\mathsf{pk},(\mathsf{psig},\mathsf{nonce}))$ を計算する。

(4) $\mathcal{R}'(y;r_{\mathcal{R}})$ を実行し、同じ pk を得る。$(\mathsf{rsk}',\mathsf{rpk}') \leftarrow \mathsf{RKeyGen}(\lambda)$ を生成し、$\mathcal{R}'$ から $(\mathsf{psig}',\mathsf{nonce}')$ を取得する。

(5) $(\mathsf{m}',\mathsf{sig}') \leftarrow \mathsf{Obtain}(\mathsf{rsk}',\mathsf{pk},(\mathsf{psig}',\mathsf{nonce}'))$ を計算する。

(6) $\mathcal{R}'$ を中止し、$(\mathsf{m},\mathsf{sig}),(\mathsf{m}',\mathsf{sig}')$ を $\mathcal{R}$ に渡す。

(7) $\mathcal{R}$ が y に対して出力する解 x' を返す。

$\mathcal{R}^{\mathcal{A}^{\Sigma_c}}$ を理想的攻撃者 $\mathcal{A}^{\Sigma_c}$ を実行する帰着、$\mathcal{R}^{\mathcal{M}}$ をメタ帰着攻撃者を実行する帰着とする。補題 3 によれば、理想的攻撃者は高確率で勝利する。我々は次を示す：

$$\left|\Pr[\mathsf{Succ}(\mathcal{R}^{\mathcal{A}^{\Sigma_c}})]-\Pr[\mathsf{Succ}(\mathcal{R}^{\mathcal{M}})]\right| = \mathsf{negl}(\lambda)$$

これは計算的秘密鍵独立性ゲームへの帰着によって示される。

秘密鍵独立性ゲームに対する攻撃者 $\mathcal{R}^{\Sigma_c}$ を次のように構成する：

(1) ゲームから $\mathsf{rpk}_0,\mathsf{rpk}_1$ を受け取り、$y \leftarrow I(\lambda)$ を生成す

る。$\mathcal{R}(y; r_{\mathcal{R}})$ を実行して pk を得る。

(2) rpk_0 を用いて $\mathcal{R}$ を実行し、$(\mathsf{psig}, \mathsf{nonce})$ を得る。

(3) $\mathcal{R}'(y; r_{\mathcal{R}})$ を実行し、rpk_1 を用いて $(\mathsf{psig}', \mathsf{nonce}')$ を取得する。

(4) $(\mathsf{pk}, \mathsf{psig}, \mathsf{nonce}, \mathsf{psig}', \mathsf{nonce}')$ をゲームに出力する。

(5) ゲームから $(\mathsf{m}, \mathsf{sig}, \mathsf{m}_b, \mathsf{sig}_b)$ を受け取り、$\mathcal{R}$ に渡して x' を得る。

(6) $b' \leftarrow V(x', y)$ を計算し、ゲームに出力する。

$b = 0$ の場合、このシミュレーションは理想的攻撃者 $\mathcal{A}^{\Sigma_c}$ に対応し、$b = 1$ の場合、メタ帰着 $\mathcal{M}$ に対応する。$\mathsf{Succ}(Z)$ を $\mathcal{R}^Z$ が y を解く事象とすると：

$$\Pr[\mathsf{Succ}(\mathcal{A}^{\Sigma_c})] - \Pr[\mathsf{Succ}(\mathcal{M})] = \mathbf{Adv}^{\mathsf{cskind}}_{\mathsf{NIBS},\mathcal{R}^{\Sigma_c}}(\lambda).$$

補題 4 より、NIBS は計算的秘密鍵独立性を満たす。したがって：

$$\Pr[\mathsf{Succ}(\mathcal{A}^{\Sigma_c})] = \Pr[\mathsf{Succ}(\mathcal{M})] + \mathsf{negl}(\lambda).$$

さらに補題 3 により $\Pr[\mathsf{Succ}(\mathcal{A}^{\Sigma_c})] = 1 - \mathsf{negl}(\lambda)$ であるから、

$$\Pr[\mathsf{Succ}(\mathcal{M})] = 1 - \mathsf{negl}(\lambda),$$

が成り立つ。これは $\mathcal{R}$ が単純帰着を用いて問題を解くという仮定と矛盾する。 □

参考文献

[1] Baldimtsi, F., Cheng, J., Goyal, R. and Yadav, A.: Non-Interactive Blind Signatures: Post-Quantum and Stronger Security, *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part II* (Chung, K. and Sasaki, Y., eds.), Lecture Notes in Computer Science, Vol. 15485, Springer, pp. 70–104 (2024).

[2] Baldimtsi, F. and Lysyanskaya, A.: Anonymous credentials light, *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 1087–1098 (2013).

[3] Canard, S., Gaud, M. and Traoré, J.: Defeating malicious servers in a blind signatures based voting system, *International Conference on Financial Cryptography and Data Security*, Springer, pp. 148–153 (2006).

[4] Chaum, D.: Blind Signatures for Untraceable Payments, *CRYPTO*, pp. 199–203 (1982).

[5] Chaum, D.: Blind signature system, *Advances in Cryptology: Proceedings of Crypto 83*, Springer, pp. 153–153 (1983).

[6] Hanzlik, L.: Non-interactive Blind Signatures for Random Messages, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V* (Hazay, C. and Stam, M., eds.), Lecture Notes in Computer Science, Vol. 14008, Springer, pp. 722–752 (2023).

[7] Hanzlik, L., Paracucchi, E. and Zanotto, R.: Non-interactive Blind Signatures from RSA Assumption and More, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II* (Fehr, S. and Fouque, P., eds.), Lecture Notes in Computer Science, Vol. 15602, Springer, pp. 365–394 (2025).

[8] Heilman, E., Alshenibr, L., Baldimtsi, F., Scafuro, A. and Goldberg, S.: TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub, *24th Annual Network and Distributed System Security Symposium, NDSS 2017, San Diego, California, USA, February 26 - March 1, 2017*, The Internet Society (2017).

[9] IETF: Privacy Pass (privacypass). https://datatracker.ietf.org/wg/privacypass/documents/.

[10] Kazuki Yamamura, T. O. and Fujisaki, E.: On Non-Interactive Blind Signatures in the Plain Model Using Complexity Leveraging (2025). To apper in "Financial Cryptography and Data Secuirty 2025".

[11] Morgan, A. and Pass, R.: On the Security Loss of Unique Signatures, *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part I* (Beimel, A. and Dziembowski, S., eds.), Lecture Notes in Computer Science, Vol. 11239, Springer, pp. 507–536 (2018).

[12] Pass, R.: Limits of provable security from standard assumptions, *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011* (Fortnow, L. and Vadhan, S. P., eds.), ACM, pp. 109–118 (2011).

[13] Zhang, H., Chen, X. and Huang, Q.: Lattice-Based Non-interactive Blind Signature Schemes in the Random Oracle Model, *Provable and Practical Security - 18th International Conference, ProvSec 2024, Gold Coast, QLD, Australia, September 25-27, 2024, Proceedings, Part I* (Liu, J. K., Chen, L., Sun, S. and Liu, X., eds.), Lecture Notes in Computer Science, Vol. 14903, Springer, pp. 289–308 (2024).