修士論文

# モノの電子署名：
# サイバーフィジカル系における暗号学的手法

# Signature for Objects: Cryptographic Methods in Cyber-Physical Systems


指導教員　　松浦幹太　教授

東京大学大学院 情報理工学系研究科 電子情報学専攻

48-206446　　林リウヤ


令和 4 年 1 月 27 日提出

# 内容梗概

近年サプライチェーンセキュリティへの関心が高まっている．内閣府は戦略的イノベーション創造プログラムで課題の一つとして「IoT 社会に対応したサイバー・フィジカル・セキュリティ」を挙げており，サプライチェーン全体のセキュリティを実現するために「信頼の創出・証明」技術が重要だと述べている．本研究はまさしくサプライチェーンにおける信頼の証明手法について検討したものである．

取引の信頼を証明するためには証明書に相当するものを以て取引を検証できることが重要である．たとえばアリスとボブの通信において，そのままではアリスが受け取ったメッセージが誰から送られたものか分からない．そこで電子署名方式では，正しくボブが送信したものであると検証できるようにするためにボブはメッセージのダイジェスト値に自身の署名鍵で署名などする．これにより，メッセージを受け取ったアリスはボブの検証鍵を用いてその正当性を検証することができるようになる．この電子署名の技術を，サイバー空間だけでなく現実世界の物体が登場するようなサイバーフィジカル系においても同様に活用することができれば，各取引の正当性を検証できるようになることが期待される．つまり，この技術を活用することでサプライチェーン全体のセキュリティの実現に大きく近づく．

しかし，既存の電子署名の技術は全てサイバー空間で閉じており，サイバーフィジカル系に拡張された暗号技術は現時点ではほとんど存在しない．また，サイバーフィジカル系のセキュリティに関する研究は多く存在する一方で，既存研究は特定のシステムや製品に関する議論であるか安全性の議論がヒューリスティックなものにとどまっている．

そこで本研究では，物体への操作を定式化することで暗号学的基盤を物理空間へ拡張し，これを用いて物体に署名する手法である「モノの電子署名」を提案した．物体への操作は物体を加工・生成するコマンドと，画像など対応する電子データを得るセンシングに分けられ，それぞれ各操作を表すオラクルを方式に与えることで物理空間での操作が可能なアルゴリズムを導入した．センシングにより物体に対応する電子データを得られるようになったため，その電子データに対して従来の電子署名を用いることができるようになる．このように作成された署名は，基盤とする電子署名方式が EUF-CMA 安全であるならば，物理空間での操作が可能な攻撃者に対して定義された安全性 (EUF-COA) を満たすことが示された．また，モノの電子署名特有の問題として，署名のみを手に入れた攻撃者が署名から物体を推測することで偽造に活用される恐れがあることを指摘した．この攻撃に対する安全性をモノの秘匿性として定義し，それを満たす構成も示した．

# 目次

# Chapter 1　序論

## 1.1　研究背景

**社会的背景．**　近年のサプライチェーンのグローバル化に伴い，サプライチェーン自体が非常に大きく複雑なものになってきている．この影響によりサプライチェーン全体を詳細に管理することが困難であるという現状がある．また，サプライチェーンにおける情報交換の大部分がサイバー空間に移行しており，情報の改竄や漏洩といったサイバー空間でのインシデントがサプライチェーンに直接影響を与えることも少なくない．こうしたサプライチェーンセキュリティへの関心の高まりは，内閣府が戦略的イノベーション創造プログラムで課題の 1 つとして「IoT 社会に対応したサイバー・フィジカル・セキュリティ」を挙げていることからもわかる．内閣府が公開しているレポート [45] の中でサプライチェーン全体のセキュリティを実現するために「信頼の創出・証明」技術が重要だと述べられている．我々は特に，製品などの物体が関わる取引における「信頼の創出・証明」技術を研究対象としている．

より具体的な社会課題としては，あらゆる機器や製品の偽造が急速に拡大していることが挙げられる．OECD[1]のレポート [32] によると，例えば貿易において，全世界の取引の 3.3%が偽造品や海賊版にあたり，その総額は 5090 億米ドルに及ぶ．これは技術の発展に伴い，専門家でも偽造品と本物の区別がつかないほど偽造の精度も向上していることが原因の 1 つである．偽造品が一切登場しないと信頼されるサプライチェーンが登場することで，意図せず偽造品を手に入れる機会が減り，偽造品の流出も抑制することができると考えられるため，信頼できるサプライチェーンの構築を急ぐ必要がある．

**物体に対する電子署名の必要性．**　信頼できるサプライチェーンを実現するうえで，各製品の素材や部品が正規なものであることを工程を遡って検証できる機能が求められる．また，上記の通りそのような検証のために使用される情報の多くはサイバー空間上で伝達されていくことが想定される．その際，素朴な手法として，委託先が発注元へ注文品を送付するときに，その品は正しく発注元が依頼したものであると電子署名を付ける，という方法が考えられる．しかし，そのような電子署名が注文品の各部品と直接的に紐づけられていない限り，部品のすり替えは容易であり，信頼できるサプライチェーンの実現は困難である．したがって，物理的な物体に対して直接電子署名を作成することが求められるが，電子署名は電子データに対してのみ生成可能であるため，物理空間に対しても適用可能となるような電子署名の拡張が必要となる．本稿では，そのような拡張がなされた電子署名を「**モノの電子署名**」と呼ぶことにする．

[1]European Organization for Economic Cooperation and Development

**厳密な暗号学的アプローチの重要性．**　モノの電子署名を実現するアプローチは，直観的にはすぐにいくつか思い浮かぶものの，これらの直観的な手法の厳密な安全性評価を行うことは難しい．例えば，従来の電子署名と既存の物体同一性判定アルゴリズムを組み合わせることで容易に構成できるように見えるが，既存の暗号理論の枠組みでは安全性評価が困難である．なぜなら，暗号理論においては一部の例外を除き，ほとんどの技術が電子データのみを取り扱い可能なモデル化が為されており，電子署名においてもそのような前提がなされているからである．そのため，モノの電子署名を実現するためには，そもそも電子データ以外も取り扱いが可能な暗号理論的枠組みの構築が不可欠であり，すなわち，基盤的理論の構築にまで立ち返る必要がある．本研究でも，そのような基盤的理論の構築を主眼においており，また，この枠組みにおいて直観的な手法の安全性を厳密に評価することを目的としている．

## 1.2　証明可能安全性

**計算量的仮定を用いた安全性証明．**　前節の最後で暗号理論の枠組みを用いて厳密に安全性を評価することが目的だと述べた．ここではまず厳密な安全性評価とは何を指すのかを記す．暗号理論的に安全だと言われているものは，その全てに安全性証明がつけられている．この証明では，計算量的に解くとこが困難であるとされている素因数分解問題や離散対数問題などの存在（計算量的仮定）を用いる．方式の安全性を破るアルゴリズムが存在するならば，そのアルゴリズムがある計算量的仮定を破るので矛盾することを示し，対偶よりその計算量的仮定から方式の安全性を証明する．例えば，計算量的仮定の 1 つである DDH 仮定が困難であるならば，ElGamal 暗号は IND-CPA 安全である，というように安全性証明がつけられる．

**一般的構成法 (General Construction)．**　上のような安全性証明の手法を帰着による安全性証明という．帰着を用いた安全性証明は，その帰着先に標準的な計算量的仮定だけでなく既に安全性証明がなされた様々な方式の安全性を用いることができる．この例を次に示す．詳細は 3 章に記すが，電子署名の安全性として EUF-CMA 安全性というものが存在する．EUF-CMA 安全な構成は既にいくつか知られており，一般に EUF-CMA 安全な電子署名方式は存在を仮定しても問題はない．すなわち，ある方式について新たな安全性を定義した場合には，安全性証明に「その安全性を破るアルゴリズムが存在するならば，そのアルゴリズムを用いて基盤とする電子署名方式の EUF-CMA 安全性を破るアルゴリズムが構成できる」ということを示せばよい．以上のように，既に安全性証明がなされた様々な方式の安全性を用いてその構成をブラックボックス的に扱い，存在を仮定して新たな方式の構成を提案する手法を一般的構成法という．一般的構成法は暗号理論において非常に大きな役割を占めており，この手法により数多の安全性定義やそれを満たす構成の証明がなされている．本研究においても，提案する方式の安全性を電子署名方式の安全性に帰着させて考えており，電子署名方式自体はブラックボックスとして扱う．

## 1.3　本研究の貢献

**物理空間に拡張された暗号学的モデル化．**本研究の主な貢献は，物理空間とサイバー空間をつなぐために物体を暗号学的に定式化し，これを用いて「モノの電子署名」という概念を提案することにある．既存の暗号理論では電子データを対象とし，暗号方式や署名方式に対して様々な攻撃者を考えることでその安全性を定義している．一方で実在物体を考える際には，物体を暗号学的にモデル化し，それを用いて攻撃者が取りうる行動を定式化することでようやく暗号学的に安全性定義が可能になる．物体の暗号学的なモデル化に際して，本研究では既存のアルゴリズムを拡張した概念である PEA (Physically Enhanced Algorithm) を提案する．PEA は，物体の集合と各物体に対する操作を表すオラクルが与えられたときに，それらを用いて物理空間での行動を記述するアルゴリズムである．この PEA を用いると攻撃者が行う物理空間での行動を定式化することができるため，物理的な行動を取る攻撃者に対しても安全性定義が可能になり，これにより初めて安全性が証明可能な「モノの電子署名」を実現するうえでの枠組みが確立できる．本研究においては PEA の概念を厳密に定義し，その枠組みにおいて (1) 物体の操作に関する暗号学的定式化，および (2) 厳密に安全性を証明可能なモノの電子署名の具体的構成，に関して議論を行う．また，本研究で提案するモノの電子署名に関して従来の電子署名と異なる性質を持つために新たな安全性定義としてモノの秘匿性を導入する必要があることを発見した．それに伴い (3) モノの電子署名特有の問題，および (4) モノの秘匿性の安全性定義とそれを満たす構成，に関して議論を行う．

**物体の操作に関する暗号学的定式化．**　物体への操作は，物体を加工する操作と物体を電子データに変換する操作に分けられる．本稿では前者をコマンド，後者をセンシングと呼ぶ．両者とも物体を直接触る操作であり，それ自体をビット列で表現できないため，各操作をオラクルとして表現する．すなわち，各オラクルはコマンドの 1 つかセンシングの 1 つの役割を持っており，物体を入力に取ることでそのオラクルに応じた操作を行う．これらの操作を定式化するために，操作の対象となる物体を定義する必要がある．ここでは操作の対象とする物体の集合 $\mathbb{X}$ が方式に予め与えられているものとする．これは従来の電子署名方式におけるメッセージ空間に相当する．コマンドは決定的な操作とし，実行するコマンドオラクルと対象となる物体を選ぶと一意に新たな物体が生成される．このとき，本研究ではコマンドに入力された物体は無くならないものとして定式化している．一見すると入力物体が無くなる定式化が自然だが，本質的には等価となるため問題は無い．センシングは非決定的な操作とするが，同一のセンシングに対して異なる物体を入力とすると必ず異なる電子データを返す，という理想的な性質を満たすとする．より厳密に記述すると，異なる 2 つの物体 $A, B$ を考え，センシングを行ったときに出力される電子データの空間をそれぞれ $S_A, S_B$ と置くと，必ず $S_A \cap S_B = \emptyset$ が成立する．このため，少なくとも電子データの空間の大きさはコマンドで作成しうる物体の数より大きい必要がある．詳細な議論は 4 章で行う．以上のように，オラクルを用いて物体への操作を定式化することで PEA の定義が可

能となる．

**厳密に安全性を証明可能なモノの電子署名の具体的構成．**　本研究では，PEA でモデル化された利用者および攻撃者に基づき安全性定義を行い，また，この安全性定義のもとで安全となる方式の具体的な構成について明らかにする．基本的な電子署名の安全性概念である偽造不可能性に関しては，通常の電子署名方式と同様に EUF (Existential Unforgeability) を考えるが，攻撃者がクエリするものが単なる電子データでないため CMA (Chosen Message Attacks) ではない．その代わりに，攻撃者は物体の署名と電子データをクエリすることができ，また攻撃者が持つ物体に対して任意のコマンドを実行することができるものとしている．このような攻撃者に対しても，署名をクエリしたことがない物体の署名が偽造できないという安全性を EUF-COA (Existential Unforgeability under Chosen Object Attacks) として定義している．また，モノの電子署名の安全性を満たす構成には，センシングより得られた電子データが 2 つ与えられたときに，それぞれの電子データについて入力とした物体が同じものであるかを判定する関数が必要となる．本研究では，これを Relation Function と呼ぶ．すなわち，同一の物体をセンシングすることで得られる 2 つの電子データを入力とすると Relation Function は 1 を返し，その逆も成立する．5 章では，この Relation Function と通常の電子署名方式を組み合わせることでモノの電子署名を構成する手法を提案する．そして，センシングや Relation Function が理想的な性質を満たし，かつ通常の電子署名方式が PEA 攻撃者に対して EUF-CMA 安全であるという条件の下で，構成されるモノの電子署名方式が EUF-COA を満たすことを示す．

**モノの電子署名方式特有の問題．**　EUF-COA 安全性を満たすだけでは以下で示す問題を解決することはできない．メッセージに署名する従来の電子署名方式では，通常メッセージと署名を結合してサイバー空間で送信する．そのため，署名からメッセージが特定できない，といった安全性を考える必要がない．一方，モノの電子署名方式における署名は，物体にセンシングを実行することで対応する電子データ（以下センシングデータ）を得た後にセンシングデータを入力としてアルゴリズムを実行することで生成される．署名後は物理空間で物体を，サイバー空間で署名をそれぞれ検証者に送る．このとき，署名から物体の情報が得られると，署名を得た攻撃者がその情報をもとに物体を生成することで，生成した物体と得た署名の組が検証を通過してしまう可能性がある．これは EUF-COA 安全性では対応しきれない偽造攻撃であり，かつモノの電子署名方式特有の問題である．

**モノの秘匿性の安全性定義とそれを満たす構成．**　本研究の貢献の 1 つは，上に述べたモノの電子署名特有の問題を発見し，対策としてモノの電子署名方式で署名から対応する物体が特定できないことを示す**モノの秘匿性**という安全性を提案することにある．現実世界で考えると，サイバー空間にて物体の署名を得た悪意のある人が，世にある全ての物体からその物体を特定することが困難である，という安全性を指し示す．これは，方式の対象とする物体集合のサイズが小さい場合には自明に成立しない．な

ぜならば，公開である検証アルゴリズムを総当たりで実行することで容易に署名から対応する物体が特定できるからである．ゆえに，少なくとも物体集合は十分大きい（多項式より大きい）必要がある．現実にはあらゆる物体（製品）が存在し，方式の対象とする物体集合は十分大きいと考えられるため，この仮定は現実世界では問題にならない．

モノの秘匿性に対する攻撃者は PEA でモデル化されている．すなわち，物体の署名と電子データをクエリすることができ，また攻撃者が持つ物体に対して任意のコマンドを実行することができる．攻撃者は十分大きい物体集合上の分布を作成し挑戦者に送る．挑戦者は与えられた物体の分布に従って 1 つ物体を選び，その署名を攻撃者に送る．このとき，どのような PEA 攻撃者に対しても分布の最小エントロピーが十分大きい場合は署名に対応する物体が特定できない，という安全性をモノの秘匿性として定義している．モノの秘匿性を満たすために，センシングに対して追加で必要な要件は登場しない．すなわち，センシングデータから対応する物体が一意に特定できるようなセンシングを用いたとしても，安全性要件さえ満たしていればモノの秘匿性を満たすことができる．6 章では安全性定義を提案すると同時に，それを満たす具体的な構成についても明らかにする．方式は通常の電子署名方式と Relational Hash を組み合わせることで実現できる．Relational Hash は確率的ハッシュの組であり，異なる確率的ハッシュ値の組からその原像の組が与えられた関係を満たすか検証ができる方式である．詳細は 3 章に記す．センシングが理想的な性質を満たすとき，通常の電子署名方式が PEA 攻撃者に対して EUF-CMA 安全であり確率的ハッシュ関数が衝突困難性を満たすならば構成されるモノの電子署名方式が EUF-COA 安全性を満たし，また Relational Hash が偽造不可能性を満たすならば構成される方式がモノの秘匿性を満たすことを示す．

## 1.4　本稿の構成

以下，2 章では関連研究を紹介する．3 章では，はじめに諸定義について説明したのち，提案方式の安全性の基盤となる電子署名方式や確率的ハッシュ，Relational Hash について説明する．4 章では，モノの電子署名の実現に必要である物体への操作を定式化する手法を説明する．5 章では，モノの電子署名の簡単な構成と，その安全性が基盤とする電子署名方式の安全性に帰着できることを示す．6 章では，モノの秘匿性を満たすモノの電子署名の構成と，その安全性証明を示す．7 章では，安全性証明で用いた仮定に関する考察を行う．8 章は本稿の結論である．

# Chapter 2　関連研究

**サプライチェーンセキュリティ．**　以前は主に経済学の分野でサプライチェーンの研究が盛んになされており，物流の効率の向上などに関する研究が主流であった．しかし2001年9月11日に起きた悲惨なテロ事件以降，サプライチェーンのセキュリティについても大きな関心が集まるようになった．Leeら [24] は，既に成功していた総合品質管理の手法から教訓を得て，適切な管理と運用設計を情報技術を活用して再度行うことで，より安全なサプライチェーンを低コストで実現できることを示した．Williamsらがまとめたように [41]，近年ではブロックチェーンや機械学習といった最新技術を用いてより安全なサプライチェーンを構成するような研究がみられる．より具体的に記すと，ブロックチェーンの改竄不可能性を利用して過去の取引情報を安全に保存する研究 [29] や，Supply Chain RIsk Management (SCRM) と呼ばれるモデルの学習により危険を予測する研究 [5] などが存在する．ただし，これらの研究における安全性の議論はヒューリスティックなものであり，理論的に安全性が保証できる証明可能安全性を備えていない．

**センシングや物体認識とその応用．**　実際に物体を認識・検知する研究は，本研究においてセンシングやRelation Functionとして定式化を行った部分に大きく関わる．Ishaiら [20] は物体を測定する手法として測定情報からは何の情報も得られないような方法を，その性質を満たす数学的な条件を考察することで示しているが，肯定的な結果は得られていない．一方，物体認識の研究の多くは物体をカメラまたはビデオを用いて画像データに変換して扱っており，画像データの中で物体を検知する手法の研究 [44, 25] や物体のクラスまで認識する物体認識の研究 [19, 4] が主流となっている．その他にも，追跡を行うために物体毎の特徴的な記述を行う研究 [28] や，動的物体に対して複数センサを用いて同一物体の判定を行う研究 [36] など，追跡や同一性判定に関する研究も数多く存在する．このうち，物体毎の特徴的な記述を行う手法を物体の指紋 (Object Fingerprinting) と呼ぶが，類似した研究として PUF (Physically Unclonable Function) が存在する．PUF は Pappu [33] により提案されたもので，その物体特有のノイズ付き関数 [3] を抽出して鍵生成を行う手法である．PUF は暗号学的なプリミティブの1つではあるが，物体から鍵を抽出する手法であり，本研究で考えている物体を受け渡す状況には適合しない．情報セキュリティの観点からみると，画像処理において敵対的サンプル [13] の存在が非常に脅威となっている．これは人の目には区別がつかないが機械の認識を誤らせるような攻撃である．例えば，人には検知できない加工を「とまれ」の標識に悪意をもって行うことで機械に「進め」と認識させられる可能性が示唆されている [37]．このとき，機械が認識する物体にモノの電子署名を付与することで機械が誤った認識を検知できるようになると考えられる．このように，モノの電子署名の応用はサプライチェーンに限定されない．

**電子署名．**　電子署名の概念は Diffie と Hellman により 1976 年に初めて提唱された [14]．その後，RSA 署名 [35]，Rabin 署名 [34]，ElGamal 署名 [15] が提案され，1988 年には Goldwasser らにより攻撃者の目的や攻撃環境に応じた安全性定義がなされた [18]．その後も，Schnorr 署名 [38]，DSA 署名 [31]，ECDSA 署名 [22]，BLS 署名 [7] など，さまざまな性質を持つ署名方式の提案やその効率性を向上する構成法の提案がなされてきているが，そのどれもが電子データを対象としており物体の署名は作成できない．物理空間を対象としていない理由としては，電子データ以外を暗号学的に取り扱うことが困難であったことや，サイバーフィジカルシステムでの脅威が現在ほど大きく意識されていなかったことが考えられる．特に前者は，攻撃者のモデルを定式化することに難しさがある．従来の暗号理論ではビット列からなる平文や署名などに対して CPA (Chosen Plaintext Attack) や CMA (Chosen Message Attack) といった攻撃者のモデルを仮定して議論を進めるが，物理的な操作が可能な攻撃者を考える際には攻撃者が物体を加工したり新たな物体を生成したりするため，それらをどう定式化するか，およびどこまでの操作を攻撃者に許可するかという問題が課題となる．

**署名の否認不可能性．**　電子署名の重要な性質の 1 つに否認不可能性 (undeniable, non-repudiation) が存在する．署名自体は複製が容易であるため，署名者が署名したのにも関わらず署名していないと主張する可能性が存在する．否認不可な署名を用いることで，署名がその署名者により作成されたものであることを署名者が否認できなくなる．暗号学的にも署名の否認不可能性の安全性が定義されており [12]，特に認証システムを考える際には非常に重要な性質となっている．一方，暗号理論で署名を扱う際には否認不可能性はある種付随的な安全性であり，新たな暗号学的基盤を提案する本稿では否認不可能性に関してひとまず考慮せず，最も基本となる偽造不可能性に着目することにする[1]．

**署名の機密性・匿名性．**　Dent ら [2] により署名からメッセージが特定困難であるという機密性が，Yang ら [42] により署名から署名者が特定困難であるという匿名性がそれぞれ提案されている．Fleischhacker ら [16] は，署名が疑似乱数と識別不可能であるという疑似ランダム性を満たすならば機密性と匿名性両方の安全性を満たすことを示し，確率的ハッシュ [9, 10] と乱数抽出機 [30] を用いることで通常の電子署名方式を疑似ランダム性を満たす方式に変換できることを示した．また，さらに強力な安全性として [8] で提案されているような，より強い安全性を電子署名でも考えることもできる（詳細は**関数の秘匿性**の段落に記す）．その他にも，署名の部分情報から検証者のみが署名を復号でき，ある条件を満たした後は公開検証可能となるような署名である Conditionally Verifiable Signatures [11] や，各システムごとにユーザの仮名ドメインが存在して各ユーザはシステム側から仮名をもらうが，異なるシステム間ではその仮名が結び付けられないような署名である Domain-Specific Pseudorandom Signatures [23] など，署名から情報が漏洩しない性質を考える様々な研究が存在する．本研究で

[1] モノの秘匿性は与えられた署名を用いて署名検証が通過するような物体を特定する攻撃であり偽造不可能性に関わる安全性である．

は，メッセージに相当する部分がセンシングにより確率的な値となっているため，ファジーな値に対する電子署名方式で機密性を考慮する必要がある．

**ファジーな署名．**　Yang ら [43] によりファジーな ID を用いた署名方式や Maji ら [26] によりその一般化である属性ベース署名が，高橋ら [39] により生体情報等のファジーなデータを直接署名鍵として用いる方式が提案されている．これらではユーザの匿名性やプライバシーに関する安全性が提案されているが，いずれも対象は署名鍵・検証鍵である．本研究では署名するメッセージがファジーな値であるため，異なるアプローチが必要となる．

**関数の秘匿性．**　モノの秘匿性と類似した概念の研究として関数の秘匿性を満たす ID ベース暗号の研究が存在する [8]．これは検索可能暗号 [6] に対する攻撃手法の 1 つであるオフラインキーワード推測攻撃 [21] への対策手法として提案された．匿名 ID ベース暗号と検索可能暗号はある条件下で等価であることが知られている [1]．関数の秘匿性は，信頼できる第三者機関により作成された秘密鍵から対応する ID が特定できない，という安全性を表す．より具体的には，ある分布からサンプルされた ID を用いて作成された秘密鍵から，その分布が攻撃者が作成した分布なのか一様分布なのか特定することが困難である，という定義になる．より強いモノの秘匿性を考える場合には，関数の秘匿性の定義のように，物体の分布が攻撃者が作成した分布なのか一様分布なのかを署名から特定することが困難である，という安全性を考えることができる．

**ゼロ知識証明．**　電子署名とゼロ知識証明 [17] を組み合わせることにより，署名が正当であること以外の情報を漏らさず署名検証が可能な方式が存在する．情報を秘匿するという点でモノの秘匿性の達成にもゼロ知識証明の応用が考えられるが，今回の場合は適さない．なぜならば，署名検証で検証者が用いる情報は物体から得られるセンシングデータであり確率的な値となる．また，その値がなければ検証できないような方式を考えているため，対話が必要になるからである．検証者が得るセンシングデータなしにゼロ知識証明を作成する場合には，署名する物体のセンシングデータがある範囲内に収まることの証明を付ける必要があるが，これではモノの秘匿性を満たせない．

# Chapter 3　準備

## 3.1　基本的概念

**表記.**

- 自然数を $\mathbb{N}$，整数を $\mathbb{Z}$ で表す．$p \in \mathbb{N}$ が与えられたとき，$\{x \mid \forall z \in \mathbb{Z}; x = z \bmod p\}$ を $\mathbb{Z}_p$ で表す．すなわち，$\mathbb{Z}_p = \{0, 1, \cdots, p-1\}$．また，$\mathbb{Z}_p \setminus \{0\}$ を $\mathbb{Z}_p^*$ で表す．すなわち，$\mathbb{Z}_p^* = \{1, \cdots, p-1\}$.
- 計算モデルとしてチューリングマシン（以下 TM）を考える．ある問題 $\Sigma$ の解を見つけることができるオラクル $O_\Sigma$ が存在したとき，自身で計算可能か問わず問題をオラクルに問い合わせて（= クエリして）その解を得られる TM をオラクルチューリングマシンを（OTM）と呼ぶ.
- 確率的多項式時間アルゴリズム（Probabilistic Polynomial-Time Algorithm）を PPTA で表す．PPTA 攻撃者とは任意の PPTA が実行可能な攻撃者である.
- 2 つの関数 $f, g$ について，$f(x) = O(g(x))$ とは $f$ が $g$ に漸近的に上から抑えられることを意味する
- ある $\lambda \in \mathbb{N}$ が与えられたとき，$poly(\lambda)$ は $\lambda$ の多項式で表現できる値を指す．すなわち，$poly(\lambda) = \{x \mid \exists c \in \mathbb{N}; x = O(\lambda^c)\}$．また，$negl(\lambda)$ は十分大きい $\lambda$ に対して $\frac{1}{poly(\lambda)}$ よりも小さい値を指す．どんな PPTA も解を求められる確率が $negl(\lambda)$ 以下であるとき，解を求めることはできないものとみなす.
- $\mathcal{X}$ を集合 $X$ 上の確率分布とし，$x \in X$ が $\mathcal{X}$ からサンプルされる確率を $\mathcal{X}(x)$ で表すとする．このとき，分布 $\mathcal{X}$ の最小エントロピー $H_\infty(\mathcal{X})$ は以下の式で定義される：$H_\infty(\mathcal{X}) := \min_{x \in X}\{-\log(\mathcal{X}(x))\}$．$k$-source とは $H_\infty(\mathcal{X}) \geq k$ となる分布を表す．$k$-source 攻撃者とは出力する分布が $k$-source である攻撃者を表す.
- 関数 $dist(x, y)$ は $|x| = |y|$ となる $x, y$ を入力に取り，そのハミング距離を返す.
- $\langle x_i \rangle_{i=0}^n$ は $n+1$ 個の連続した値を表す.

**双線形写像.**　$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ を乗法巡回群とする．写像 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ が双線形写像であるとは，任意の $h \in \mathbb{G}_2$ に対して $g_1 \mapsto e(g_1, h)$ が線形写像となり，かつ任意の $f \in \mathbb{G}_1$ に対して $g_2 \mapsto e(f, g_2)$ が線形写像となることである．すなわち，$f_1, g_1 \leftarrow \mathbb{G}_1, f_2, g_2 \leftarrow \mathbb{G}_2$ とすると $e(f_1, f_2) \cdot e(g_1, f_2) = e(f_1 \cdot g_1, f_2)$ および $e(f_1, f_2) \cdot e(f_1, g_2) = e(f_1, f_2 \cdot g_2)$ が成立する．これらより，任意の $r, s \in \mathbb{N}$ について $e(f_1^r, g_2^s) = e(f_1, g_2^s)^r = e(f_1, g_2)^{rs}$ が成立する．この双線形写像の計算をペアリング演算と呼ぶ．ペアリング演算の具体

的な構成としては，楕円曲線上の群演算を考えた Weil のペアリング [40] などが存在する．

**誤り訂正可能な線形符号（linear ECC）．**　誤り訂正可能な線形符号（linear Error Correcting Code: linear ECC）の定義を以下に示す．本稿では linear ECC の構成自体は研究の対象外とし，下記の性質を満たす linear ECC は存在するものとして議論を進める．具体的な誤り訂正の手法の 1 つとしては，線形符号の直交補空間の生成行列を用いて誤り訂正を行うパリティチェックなどが存在する．

**定義 3.1.** 入力空間を $\mathbb{F}_2^k$，符号語空間を $\mathbb{F}_2^n$ とする．$\mathcal{C} = (\mathrm{ENCODE}, \mathrm{DECODE})$ が $(n, k, d)$ linear ECC であるとは，$\mathcal{C}$ が以下の式を常に満たすことである：どんな入力 $x \in \mathbb{F}_2^k$，誤りベクトル $e \in \mathbb{F}_2^n$ に対しても，$dist(0, e) \leq d/2$ ならば，

$$\mathrm{DECODE}(\mathrm{ENCODE}(x) + e) = x$$

**ジェネリックグループモデル．**　ジェネリックグループモデルは暗号学的な安全性証明で用いられるモデルの 1 つで，群上の演算を理想化したモデルである．このモデルでは，群の要素は全て無意味なシンボルで表され，オラクルに 2 つの群を表すシンボルをクエリすることで，その演算結果に応じたシンボルを受け取ることができる．素因数分解問題や離散対数問題などの標準仮定の計算量的な解析や，新たに仮定を導入する場合の困難性の証明などに用いられる．本稿では，7 章にて Decisional Binary Mix 仮定の困難性を示すためにジェネリックグループモデルを導入している．

## 3.2　電子署名方式

**シンタックス．**　$\mathbb{M} = \{0,1\}^*$ をメッセージ空間とする[1]．あるメッセージ $m \in \mathbb{M}$ に署名を作成する電子署名方式は以下の 3 つの PPTA の組 $(\mathsf{DS.KG}, \mathsf{DS.Sign}, \mathsf{DS.Ver})$ から構成される：

- $\mathsf{DS.KG}(1^\lambda) \to (pk, sk)$ ：鍵生成アルゴリズム．セキュリティパラメータ $1^\lambda$ を入力として受け取り，検証鍵 $pk$，署名鍵 $sk$ を出力する．
- $\mathsf{DS.Sign}(sk, m) \to \sigma$ ：署名生成アルゴリズム．署名鍵 $sk$，メッセージ $m$ を入力として受け取り，署名 $\sigma$ を出力する．
- $\mathsf{DS.Ver}(pk, m, \sigma) \to \{0,1\}$ ：署名検証アルゴリズム．検証鍵 $pk$ とメッセージ $m$，署名 $\sigma$ を入力として受け取り，0 または 1 を出力する．

次の式が成立するとき，電子署名方式は正当性を満たすという：

$$\text{for all } \lambda, \text{ for all } m \in \mathbb{M}, \text{ if } (pk, sk) \leftarrow \mathsf{DS.KG}(\lambda),\ \sigma \leftarrow \mathsf{DS.Sign}(sk, m),$$
$$\text{then we have } \mathsf{DS.Ver}(pk, m, \sigma) = 1$$

[1] 一般に電子署名はセキュリティパラメータに依存したメッセージ空間に対して定義されることが多いが、そのような場合でも衝突困難性ハッシュを仮定すればメッセージ空間を $\{0,1\}^*$ に広げることが可能である．

**安全性定義．**　電子署名方式の安全性として EUF-CMA（Existential Unforgeability under Chosen Message Attacks）を定義する．これは，複数のメッセージについて正しい署名を見ることができる攻撃者でも，署名検証を通過するような新たなメッセージと署名のペアの偽造ができない，という安全性を表す．

より厳密な定義を記述する．$A$ を任意の PPTA が実行可能な攻撃者とする．$A$ の攻撃成功確率を $\mathrm{Succ}_A^S$ を

$$\mathrm{Succ}_A^S = \Pr\left[\begin{array}{c}(pk, sk) \leftarrow \mathsf{DS.KG}(\lambda); \\ (m, \sigma) \leftarrow A^{\mathsf{DS.Sign}(sk,\cdot)}(pk) : \\ \mathsf{DS.Ver}(pk, m, \sigma) = 1 \wedge m \notin \mathcal{M}\end{array}\right] \tag{3.1}$$

で定義する．ただし，オラクル $\mathsf{DS.Sign}(sk, \cdot)$ はクエリされたメッセージ $m$ に対して $\mathsf{DS.Sign}(sk, m)$ を実行して署名を返すオラクルであり，$A$ はこのオラクルに任意の回数メッセージをクエリしてそのメッセージに応じた署名を受け取ることができる．また，$\mathcal{M}$ はオラクルにクエリしたメッセージの集合を表す．

**定義 3.2.** 電子署名方式 $\Sigma_S = (\mathsf{DS.KG}, \mathsf{DS.Sign}, \mathsf{DS.Ver})$ が EUF-CMA を満たすとは，任意の PPTA 攻撃者 $A$ に対して上で定義した $\mathrm{Succ}_A^S$ が無視できる確率であることである．すなわち $\mathrm{Succ}_A^S \leq negl(\lambda)$ であれば，その方式は任意の PPTA 攻撃者に対して EUF-CMA 安全性を満たす．

## 3.3　確率的ハッシュ

確率的ハッシュ[9, 10] は，入力とランダムな値を用いて計算するハッシュ関数である．確率的であるため，原像とハッシュ値が正しい組であるかを検証するアルゴリズムが必要となる．以下に厳密な定義を示す．

鍵空間 $\{K_\lambda\}$，乱数空間 $\{R_\lambda\}$，出力長 $\lambda(n)$ となる確率的関数族アンサンブルとは，全ての $k \in K_\lambda$ に対して $h_k : \{0,1\}^n \times R_n \to \{0,1\}^{\lambda(n)}$ となる関数の族 $H^{(\lambda)} = \{h_k\}_{k \in K_\lambda}$ のアンサンブル $\mathcal{H} = \{H^{(\lambda)}\}_{\lambda \in \mathbb{N}}$ である．本稿では全ての確率的関数族アンサンブルが多項式時間で計算可能であるものとする．

**定義 3.3.** 確率的関数族アンサンブル $\mathcal{H} = \{H^{(\lambda)}\}_{\lambda \in \mathbb{N}}$, $H^{(\lambda)} = \{h_k\}_{k \in K_\lambda}$ は，次の 2 つの性質を満たす検証アルゴリズム $\mathsf{V}$ が存在するとき，公開検証可能であるという：ある $\lambda$ に対して

- **完全性**：全ての $k \in K_\lambda, r \in R_\lambda$ と入力 $x$ に対して常に $\mathsf{V}(k, x, h_k(x, r)) = 1$
- **衝突困難性**：どんな PPT 攻撃者 $A$ に対しても，次の式が成立するような無視可能関数 $negl()$ が存在する：

$$\Pr\left[\begin{array}{l}k \leftarrow K_\lambda; (x, y, c) \leftarrow A(k) : \\ x \neq y \wedge \mathsf{V}(k, x, c) = \mathsf{V}(k, y, c) = 1\end{array}\right] < negl(\lambda) \tag{3.2}$$

確率的ハッシュの特徴としてハッシュ値から入力の情報が一切洩れない性質を満たすことができる．この性質を完全一方向性 (POW) と呼び，特に 2 値に関する完全一方向性の定義を以下に示す．決定的なハッシュ関数では完全一方向性を満たすことができないことが知られている．

**定義 3.4.** $\mathcal{X}$ を集合 $X$ 上の確率分布とする．また，関数族 $H = \{h_k\}_{k \in K}$ が定義域 $X$ と乱数空間 $U$ を持つとする．ただし，$k$ は鍵空間 $K$ 上の分布 $\mathcal{K}$ に従って選ばれるものとする．$H$ が $\mathcal{X}, \mathcal{K}$ に関して 2-value perfect one-way (2-POW) を満たすとは，どのような PPTA 識別者 $D$ に対しても次の式を満たすことである：

$$\left| \begin{array}{c} \Pr\left[D\left(k, h_k\left(x, r_1\right), h_k\left(x, r_2\right)\right) = 1\right] \\ -\Pr\left[D\left(k, h_k\left(x_1, r_1\right), h_k\left(x_2, r_2\right)\right) = 1\right] \end{array} \right| < \mathrm{negl}(\lambda)$$

ただし，$x, x_1, x_2$ はそれぞれ独立に $\mathcal{X}$ からサンプルされ，$k$ は $\mathcal{K}$ からサンプルされ，$r_1, r_2$ は $U$ からランダムに生成されるものとする．

## 3.4 Relational Hash

Relational Hash [27] は前節の確率的ハッシュを拡張したもので，異なるハッシュ関数のハッシュ値からそれぞれの入力がある関係 $R$ を満たすかどうか検証できるハッシュ関数である．以下に厳密な定義を示す．

**定義 3.5.** $\{R_\lambda\}_\lambda \in \mathbb{N}$ を 3 つの集合 $\{X_\lambda\}_\lambda \in \mathbb{N}, \{Y_\lambda\}_\lambda \in \mathbb{N}, \{Z_\lambda\}_\lambda \in \mathbb{N}$ に関して $R_\lambda \subseteq X_\lambda \times Y_\lambda \times Z_\lambda$ で定義される関係のアンサンブルとする．ある関係 $R_\lambda$ の Relational Hash は，次の 4 つの PPTA の組 (RH.KG, $H_R$, $H'_R$, RH.Ver) から構成される：

- $\mathsf{RH.KG}(1^\lambda) \to pk$ ：鍵生成アルゴリズム．セキュリティパラメータ $1^\lambda$ を入力として受け取り，検証鍵 $pk$ を鍵空間 $K_\lambda$ から出力する．
- $H_R : K_\lambda \times X_\lambda \times RandX \to RangeX$ ：1 つ目の確率的ハッシュ関数．ただし，$RandX$ は関数 $H_R$ の乱数空間を表し，$RangeX$ はセキュリティパラメータ $1^\lambda$ が与えられたときの関数 $H_R$ の値域を表す．
- $H'_R : K_\lambda \times Y_\lambda \times RandY \to RangeY$ ：2 つ目の確率的ハッシュ関数．ただし，$RandY$ は関数 $H'_R$ の乱数空間を表し，$RangeY$ はセキュリティパラメータ $1^\lambda$ が与えられたときの関数 $H'_R$ の値域を表す．
- $\mathsf{RH.Ver}(pk, hx, hy, z) \to \{0, 1\}$ ：検証アルゴリズム．検証鍵 $pk$，2 つのハッシュ値 $hx \in RangeX, hy \in RangeY$，ある $z \in Z_\lambda$ を入力として受け取り，0 または 1 を出力する．

また，全ての $(x, y, z) \in (X_\lambda, Y_\lambda, Z_\lambda)$ に対して次の式が成立するとき，ある関係 $R_\lambda$ の Relational Hash は正当性を満たすという：$r \leftarrow RandX$, $s \leftarrow RandY$ に対して

$$\Pr\left[\begin{array}{c} pk \leftarrow \mathsf{RH.KG}(1^\lambda); \\ hx \leftarrow H_R(pk, x, r); \\ hy \leftarrow H'_R(pk, y, s) : \\ \mathsf{RH.Ver}(pk, hx, hy, z) \equiv R(x, y, z) \end{array}\right] = 1 - negl(\lambda)$$

以下では簡単のため，$R_\lambda$, $X_\lambda$, $Y_\lambda$, $Z_\lambda$ は単にそれぞれ $R$, $X$, $Y$, $Z$ で表すことがある．また，$H_R(pk, x, r)$, $H'_R(pk, y, s)$ を単に $H_R(pk, x)$, $H'_R(pk, y)$ で表すことがある．

**安全性定義**　[27] では 4 つの安全性 (One-way, Twin One-way, Unforgeability, Oracle Simulation) が定義されているが、本稿には安全性証明で用いる偽造不可能性 (Unforgeability) の定義のみ記す．

**定義 3.6.** $\mathcal{X}, \mathcal{Y}$ をそれぞれ $X, Y$ 上の確率分布とする．ある Relational Hash 方式 $\Sigma_{RH} = (\mathsf{RH.KG}, H_R, H'_R, \mathsf{RH.Ver})$ が確率分布 $\mathcal{X}, \mathcal{Y}$ に関して，次の 2 つの条件を満たすならば PPTA 攻撃者に対して偽造不可能性を満たすという：全ての $\lambda, x \leftarrow \mathcal{X}, y \leftarrow \mathcal{Y}$ に対して，$pk \leftarrow \mathsf{RH.KG}(1^\lambda), hx \leftarrow H_R(pk, x), hy \leftarrow H'_R(pk, y)$ が与えられたとき，

- 任意の PPTA 攻撃者 $A_1$ に対して次の式が成立するような無視可能関数 $negl()$ が存在する：

$$\Pr\left[\begin{array}{l} (hy', z) \leftarrow A_1(pk, hx) : \\ \mathsf{RH.Ver}(pk, hx, hy', z) = 1 \end{array}\right] < negl(\lambda) \tag{3.3}$$

- 任意の PPTA 攻撃者 $A_2$ に対して次の式が成立するような無視可能関数 $negl()$ が存在する：

$$\Pr\left[\begin{array}{l} (hx', z) \leftarrow A_2(pk, hy) : \\ \mathsf{RH.Ver}(pk, hx', hy, z) = 1 \end{array}\right] < negl(\lambda) \tag{3.4}$$

# Chapter 4　物体を計算量理論で扱う手法の検討

## 4.1　本章の概要

本章では，暗号理論的枠組みを物理空間に拡張するために物理的な操作を定式化する．特に，数多ある暗号分野の研究の知見を活用するために，帰着による安全性証明といった計算量理論の基礎となる部分は残したまま，物体を取り扱えるような拡張を行うことが目標である．本研究ではオラクルチューリングマシンの考え方を応用することで物理空間での操作を定式化する．より具体的には，物体への操作を表すオラクルを方式に与え，参加者（計算機）にそのオラクルへのアクセスを与えることで物理空間での操作が可能なアルゴリズム (PEA) を導入している．

物理空間での操作は，新たに物体を作成する「コマンド」および（写真など）物体に対応する電子データを得る「センシング」の 2 つに分けた．物体への操作を表すオラクルはすべてコマンドオラクルもしくはセンシングオラクルであり，各オラクルそれぞれが 1 つの物理的な操作を表しているものとする．本研究では，方式に与えられるオラクルのうち，1 つのみがセンシングオラクルであるとしている．これは，ある物体（製品）の取引において用いるセンシングの手法を 1 つに限定していることを意味する．そのため，サプライチェーンへの拡張を考慮する場合には方式に与えるセンシングの種類も増加させる必要があると考えられる．

## 4.2　センシング・コマンド

ここでは物体に対する操作の定義を行う．物体に対する操作はオラクルアクセスとして表す．以下では，物体集合 $\mathbb{X}$ に属する物体 $x$ に対する操作を考えるものとする．物体に対する操作は，物体を電子データに変換する操作と物体に手を加えて変化させる操作の 2 つに分けられる．前者の操作をセンシングと呼び，後者の操作をコマンドを呼ぶことにする．これらをオラクルとして記述するとそれぞれセンシングオラクルは $\mathsf{Sensing}(\boxed{\cdot})$，コマンドオラクルは $\mathsf{Command}(\boxed{\cdot})$ と表される．

センシングオラクルは物体 $x \in \mathbb{X}$ を指定されるとその電子データ $D$ を返す．このとき外部にある物体集合 $\mathbb{X}$ には何も手を加えない．センシングは非決定的な操作とするが，同一のセンシングに対して異なる物体を入力とすると必ず異なる電子データを返す，という性質を満たすとする．より厳密に記述すると，異なる 2 つの物体 $A, B$ を考え，センシングを行ったときに出力される電子データの空間をそれぞれ $S_A, S_B$ と置くと，必ず $S_A \cap S_B = \emptyset$ が成立する．このため，少なくとも電子データの空間の大きさはコマンドで作成しうる物体の数より大きい必要がある．

コマンドオラクルは物体 $x \in \mathbb{X}$ を指定されると，物体 $x$ にコマンドを作用させて新たな物体を作成する．すなわち，物体集合 $\mathbb{X}$ 自体はコマンドを実行するたびに含む物

体の数が増える．ただし，コマンドは決定的な操作であり，引数には 1 つの物体のみを取る操作とする．一見すると，コマンドの定義として，対象の物体 $x$ が $x'$ に置き換えられる定義の方が自然である．この場合，元となる物体を用意する必要がある．そこで，元となる物体の集合を $\mathbb{X}_m$，コマンド実行の対象である物体の集合を $\mathbb{X}$ とし，コマンドを次の 2 つの操作として考える：(i) $\mathbb{X}_m$ から物体を 1 つ選んで $\mathbb{X}$ に追加する．(ii) $x \in \mathbb{X}$ にコマンドを実行して $x'$ にする（このとき，$\mathbb{X}$ の大きさは不変）．しかし，この定義は前の定義と等価になるため，本稿ではコマンドの定義を「元の物体を保持したまま新たな物体を生成する操作」とする．また，物体集合の初期状態を $\mathbb{X}_m$ として，$\mathbb{X}_m$ にコマンドを $T$ 回実行して得られる物体全てを含む集合を $\mathbb{X}_T$ とする．このとき，コマンドオラクルの集合を $\mathbb{C}$ とすると，コマンドの性質より次の式が成立する：

$$|\mathbb{X}_T| \leq \frac{|\mathbb{C}|^T - 1}{|\mathbb{C}| - 1} \cdot |\mathbb{X}_m| \tag{4.1}$$

等号成立は，生成される物体が全て異なる物体であるときである．ここから明らかに $\mathbb{X}_T$ は有限集合である．

センシングオラクルおよびコマンドオラクルは，物体集合 $\mathbb{X}$ に属する物体を指定されると，それぞれのオラクルに応じた操作をその物体に対して実行する．それぞれのオラクルアクセスは次のように定義される．

**定義 4.1.** コマンドは物体に手を加えて変化させる物理的な操作であり，コマンドオラクルは次のように定義される：

$$\epsilon \leftarrow \mathsf{Command}(\boxed{x}) \quad \text{where } x \in \mathbb{X}$$

ただし $\epsilon$ は空文字列を表す．コマンドは決定的な操作であり，コマンドを実行すると対象の物体は保持されたまま新たな物体が生成される．ゆえに，物体集合の初期状態を $\mathbb{X}_m$ として，$\mathbb{X}_m$ にコマンドを $T$ 回実行して得られる物体全てを含む集合を $\mathbb{X}_T$ とすると，$\mathbb{X}_T$ は有限集合となる．

**定義 4.2.** センシングは物体を電子データに変換する物理的な操作であり，センシングオラクルは次のように定義される：

$$D \leftarrow \mathsf{Sensing}(\boxed{x}) \quad \text{where } x \in \mathbb{X}$$

センシングは非決定的な操作であり，同一物体に同一のセンシングを行っても帰ってくるセンシングデータが同一とは限らない．ただし，異なる物体のセンシングデータは必ず異なるものとする．

次に，物体が同一であることの定義を行う．物体が同一であるかそうでないかという判定は応用先のシステムによる．そこで，本稿では同一性判定オラクル isSame を用いてこれをモデル化する．

**定義 4.3.** 同一性判定オラクル isSame は 2 つの物体を対象として，同一物体である場合には 1 を返しそうでない場合には 0 を返すオラクルである．つまり，2 つの物体 $x_i, x_j$ に対して，

$$\mathsf{isSame}(\boxed{x_i}, \boxed{x_j}) = \begin{cases} 1 & \text{if } x_i \text{ and } x_j \text{ are the same.} \\ 0 & \text{otherwise.} \end{cases}$$

## 4.3 Physically Enhanced Algorithm (PEA)

従来の署名方式は全てPPTAにより記述され，その安全性も攻撃者として任意のPPTAが扱えることを考える．しかし，本研究では物理的な物体に対する署名を考えるため，PPTAを実在物体に対する操作まで拡張する必要がある．この拡張されたクラスをPhysically Enhanced Algorithm（PEA）と定義する．

**定義 4.4.** $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた Physically Enhanced Algorithm (PEA) とは，PPTAで実行可能な全てのアルゴリズムを実行可能で，かつ物体集合 $\mathbb{X}_m$ に含まれる物体をセンシングオラクル Sensing およびコマンドオラクル $\mathsf{Command} \in \mathbb{C}$ にクエリ可能であるアルゴリズムである．PEA は，物体集合の初期状態 $\mathbb{X}_m$，コマンドオラクルの集合$\mathbb{C}$，センシングオラクルSensingによってパラメタライズされている．

本稿で提案する電子署名方式は，PEA 攻撃者に対して，EUF-CMA 安全な（通常の）電子署名方式，衝突困難性を満たす確率的ハッシュ，偽造不可能性を満たすRelational Hash が必要である．そこで，これらを以下で定義する．

**定義 4.5.** 定義 3.2 ではPPTA 攻撃者に対する安全性を定義したが，$(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされたPEA攻撃者 $A$ に対しても同様に安全性を定義できる．特に，どんな PEA 攻撃者 $A$ に対しても式 (3.1) の $\mathrm{Succ}_A^S$ が無視できる確率であるとき，電子署名方式は PEA 攻撃者に対して EUF-CMA 安全であるという．

**定義 4.6.** 定義 3.3 では PPTA 攻撃者に対する安全性を定義したが，$(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされたPEA攻撃者 $A$ に対しても同様に安全性を定義できる．特に，どんな PEA 攻撃者 $A$ に対しても式 (3.2) が成立するような無視可能関数 $negl()$ が存在するとき，確率的ハッシュは PEA 攻撃者に対して衝突困難性を満たすという．

**定義 4.7.** 定義 3.6 では PPTA 攻撃者に対する安全性を定義したが，$(\mathbb{X}_T, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされたPEA攻撃者 $A$ に対しても同様に安全性を定義できる．特に，どんな PEA 攻撃者 $A$ に対しても式 (3.3) および式 (3.4) が成立するような無視可能関数 $negl()$ が存在するとき，Relational Hash は PEA 攻撃者に対して偽造不可能性を満たすという．

## 4.4 Relation Function

この節ではRelation Function $R$ を定義する．簡潔に述べると，ある物体にセンシングを行った 2 つの異なる出力 $D_i, D_j$ について，それらが同一の物体にセンシングを行った場合には1を，異なる物体であった場合には0を返すような関数 $R$ をRelation Functionと呼ぶ．同一性判定オラクル isSame は 2 つの物体が同一の物体であるかどうかを表す理想的なものであり，この性質を計算機で表現できる述語関数に落とし込んだものがRelation Functionである．

**定義 4.8.** $\mathbb{X}$ を物体集合，$\mathbb{S}$ をセンシングオラクルの集合とする．2 つの物体 $x_i, x_j \in \mathbb{X}$ と全てのセンシングオラクル $\mathsf{Sensing} \in \mathbb{S}$ について，$D_i \leftarrow \mathsf{Sensing}(\boxed{x_i}), D_j \leftarrow \mathsf{Sensing}(\boxed{x_j})$ とする．このとき，$x_i$ と $x_j$ が同一物体であるならば $R(D_i, D_j) = 1$ となるような述語関数 $R$ を Relation Function と呼ぶ．Relation Function $R$ は以下の性質を満たす：

$$\begin{gathered}\text{for all } x_i, x_j \in \mathbb{X}, \text{ all } \mathsf{Sensing} \in \mathbb{S},\\ \text{if } D_i \leftarrow \mathsf{Sensing}(\boxed{x_i}) \text{ and } D_j \leftarrow \mathsf{Sensing}(\boxed{x_j}),\\ \text{then we have } \mathsf{isSame}(\boxed{x_i}, \boxed{x_j}) = 1 \Leftrightarrow R(D_i, D_j) = 1\end{gathered}$$

上記の Relation function の性質が成立するためには，異なる 2 つの物体に対してセンシングを行ったときに異なる文字列が結果として得られなければならない．一方，式（4.1）で見たように，$T$ 回のコマンド実行によって得られる物体の種類は最大の場合 $T$ に関して指数的となる．これらのことから，$T$ 回のコマンド実行の後にセンシングを実行して得られる文字列の長さは $T$ に線形に依存しうることがわかる．

# Chapter 5　偽造不可能性に関する安全性定義 (EUF-COA) とその構成

## 5.1　本章の概要

この章では，4 章で定義した物理空間での操作が可能なアルゴリズム PEA を用いて具体的にモノの電子署名方式を提案する．方式には物理空間での操作を表すオラクルであるコマンドオラクル，センシングオラクルが与えられており，同様に与えられた物体集合に対してはそれらのオラクルを用いてのみ操作ができる．物体への操作を考えていること以外は従来の基本的な電子署名方と共通である．例えばシンタックスに関しては両者とも鍵生成アルゴリズム，署名アルゴリズム，署名検証アルゴリズムからなる．偽造不可能性に関する安全性定義として，従来の電子署名の安全性である EUF-CMA 安全性に相当するものを考える必要があるが，ここで攻撃者の取りうる動作のうち PPTA では表現できないものが出てくる．そのため，攻撃者が行う物理空間での操作に関して注意して安全性定義を行う必要がある．この安全性を満たす証明可能安全な構成は，センシングデータに署名を打つという直感的な方式であり，基盤とする電子署名方式が PEA 攻撃者に対しても EUF-CMA 安全であるならば提案方式が安全性を満たすことを示す．

## 5.2　EUF-COA の安全性定義

この節では，あらかじめ与えられた物体集合 $\mathbb{X}_m$ からコマンドにより作られた物体に署名する方式の提案および定義を行う．以下では，$\mathbb{X}_m$ にコマンドを $T$ 回以下実行して得られる物体をすべて含む物体集合を $\mathbb{X}_T$ とする．

**設定．**　$\mathbb{X}_m$ を有限の物体集合，$\mathbb{C}$ をコマンドオラクルの集合として，システムごとに 1 つのセンシングオラクル Sensing を選び，そのシステム内でセンシングを行う場合には常にオラクルとして Sensing を用いることとする．

**シンタックス．**　ある物体 $x$ に署名を作成するモノの電子署名方式 $\Pi$ は以下の 3 つの PPTA の組（SfO.KG，SfO.Sign，SfO.Ver）から構成される：

- $\mathsf{SfO.KG}(1^\lambda) \to (pk, sk)$ ：鍵生成アルゴリズム．セキュリティパラメータ $1^\lambda$ を入力として受け取り，検証鍵 $pk$，署名鍵 $sk$ を出力する．
- $\mathsf{SfO.Sign}(sk, \boxed{x}) \to \sigma$ ：物体 $x \in \mathbb{X}_T$ の署名を作成するアルゴリズム．物体 $x$ を対象に，署名鍵 $sk$ を入力として受け取り，署名 $\sigma$ を出力する．

- $\mathsf{SfO.Ver}(pk, \boxed{x}, \sigma) \to \{0,1\}$ ：署名 $\sigma$ の検証アルゴリズム．物体 $x$ を対象に，検証鍵 $pk$ と署名 $\sigma$ を入力として受け取り，0 または 1 を出力する．

次の式が成立するときモノの電子署名方式は正当性を満たすという：

$$\begin{gathered}\text{for all } \lambda, \text{ all } T, \text{ all } x \in \mathbb{X}_T, \\ \text{if } (pk, sk) \leftarrow \mathsf{SfO.KG}(\lambda),\ \sigma \leftarrow \mathsf{SfO.Sign}(sk, \boxed{x}), \\ \text{then we have } \mathsf{SfO.Ver}(pk, \boxed{x}, \sigma) = 1\end{gathered}$$

また，効率性の要件として，入力 $x \in \mathbb{X}_T$ に対して SfO.Sign と SfO.Sign の実行時間が $\lambda$ と $T$ の多項式で上から抑えられることを要求する．実行時間が $\lambda$ だけでなく $T$ に依存することを許す理由は，$x \in \mathbb{X}_T$ をセンシングして得られるデータのサイズが $T$ に依存して長くなる可能性があるためである．

**安全性定義．**　安全性として EUF-COA (Existential Unforgeability under Chosen Object Attack) を定義する．この安全性で考える攻撃者は，直接物体に触ることができないものとする．すなわち，攻撃者は物体を引数にとるアルゴリズムを実行できない．そのような攻撃者に対して，強い攻撃者を仮定するために，あらゆる物体の署名やセンシングデータを手に入れることができる攻撃者を考える．攻撃者の攻撃成功の条件としては，今まで署名を手に入れていない物体に対して，その物体と攻撃者が作った署名のペアが署名検証アルゴリズム SfO.Ver を通過することとする．この攻撃者の攻撃成功確率が十分小さいとき，そのモノの電子署名方式は EUF-COA を満たす，とする．

まず，物体に直接触ることのできない攻撃者が物体の署名やセンシングデータを手に入れる方法について述べる．攻撃者は物体に触ることはできないが物体を指し示すことはできるため，この物体へのポインタをラベルと呼ぶことにする．すなわち，攻撃者が物体 $x$ を指し示したいときは，攻撃者はラベル $l_x$ を用いることで物体 $x$ を指定できるとする．ここで，新しく 3 つのオラクル $\mathsf{Adv.Sign}(sk, \cdot)$，$\mathsf{Adv.Sensing}(\cdot)$，$\mathsf{Adv.Command}(\cdot)$ を考える．これら 3 つのオラクルは攻撃者が利用できるオラクルであり，ラベルをクエリすることでそれぞれのオラクルに応じたレスポンスを得られる．例えば物体 $x$ のラベルが $l_x$ であった場合，$\mathsf{Adv.Sign}(sk, l_x)$ は物体 $x$ の署名を返し，$\mathsf{Adv.Sensing}(l_x)$ は物体 $x$ のセンシングデータを返し，$\mathsf{Adv.Command}(l_x)$ は物体 $x$ に対してコマンドを実行する．

次に攻撃者の動作を定義する．攻撃者は初期状態として，物体集合 $\mathbb{X}_A$，コマンドオラクルの集合 $\mathbb{C}$，センシングオラクル Sensing をもっており，物体 $x \in \mathbb{X}_A$ の署名または電子データをオラクルに問い合わせるか，物体 $x \in \mathbb{X}_A$ に $\mathsf{Command} \in \mathbb{C}$ を実行して新たな物体を作成し，$\mathbb{X}_A$ に加えることができる．これらの動作を許された攻撃者 $A$ はラベルと署名のペア $(l_{x_A}, \sigma_A)$ を出力する．この出力に関して，$D_A \leftarrow \mathsf{Sensing}(\boxed{x_A})$ としたとき，

$$\mathsf{SfO.Ver}(pk, \boxed{x_A}, \sigma_A) = 1 \wedge R(D_A, D_i) = 0 \text{ for all } D_i \in \mathcal{D}$$

を $A$ の勝利条件とする．ただし $R$ は定義 4.8 の Relation Function であり，$\mathcal{D}$ は攻撃者が署名をリクエストした物体をセンシングして得られた電子データの集合である．
これをゲームとして記述すると以下のようになる：

***Setup.*** あらかじめ物体集合 $\mathbb{X}_A$，コマンドオラクル集合 $\mathbb{C}$，センシングオラクル Sensing は与えられているものとする．はじめに挑戦者は鍵生成アルゴリズム SfO.KG を実行して鍵ペア $(pk, sk)$ を作成し，検証鍵 $pk$ を攻撃者に渡す．ただし，$\mathbb{X}_A$ は方式構成時に与えられる物体集合 $\mathbb{X}_m$ と同じものとする．

***Actions.*** 攻撃者 $A$ は各物体 $x \in \mathbb{X}_A$ を指し示すものとしてラベル $l_x$ をもつ．このラベル情報は挑戦者にも共有される．以下の 3 つの動作を実行できる．(i) 1 つは，物体 $x \in \mathbb{X}_A$ に任意のコマンド $\mathsf{Command} \in \mathbb{C}$ を実行して新たな物体を作成する，という動作である．攻撃者は作成した物体にラベルを付与し，物体を集合 $\mathbb{X}_A$ に加える．コマンド実行ごとに新規物体のラベル情報は挑戦者に共有される．(ii) 1 つは，オラクル $\mathsf{Adv.Sensing}(\cdot)$ にラベル $l_x$ をクエリして物体 $x \in \mathbb{X}_A$ の電子データを得る，という動作である．(iii) 1 つは，オラクル $\mathsf{Adv.Sign}(sk, \cdot)$ にラベル $l_x$ をクエリして物体 $x \in \mathbb{X}_A$ の署名を得る，という動作である．ただし，署名オラクルが物体 $x$ の署名を返すたびに挑戦者は電子データ $D \leftarrow \mathsf{Sensing}(\boxed{x})$ を保存する．保存した電子データの集合を $\mathcal{D}$ とする．

***Forgery.*** 攻撃者 $A$ は物体 $x_A$ を指し示すラベル $l_{x_A}$ と署名 $\sigma_A$ の組を出力する．

A の勝利条件は $l_{x_A}$ および $D_A \leftarrow \mathsf{Sensing}(\boxed{x_A})$ について以下の式が成立することとする：

$$\mathsf{SfO.Ver}(pk, \boxed{x_A}, \sigma_A) = 1 \wedge R(D_A, D_i) = 0 \text{ for all } D_i \in \mathcal{D}$$

**定義 5.1.** 上に記述したゲームにおける攻撃者 $A$ の攻撃成功確率を $\mathrm{Succ}_A^O$ とする．モノの電子署名方式 $\Pi$ = (SfO.KG,SfO.Sign, SfO.Ver) が EUF-COA を満たすとは，$(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた任意の PEA 攻撃者 $A$ に対して $\mathrm{Succ}_A^O$ が無視できる確率であることである．すなわち $\mathrm{Succ}_A^O \leq negl(\lambda)$ であれば，その方式は $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA 攻撃者に対して EUF-COA を満たす．

## 5.3　EUF-COA を満たす構成

前節で定義したモノの電子署名方式を，通常の電子署名と Relation Function を組み合わせることで構成し，その安全性証明を行う．通常の電子署名方式を $\Sigma_S$ = (DS.KG, DS.Sign, DS.Ver) とし，物体集合 $\mathbb{X}_m$，コマンドオラクル集合 $\mathbb{C}$，センシングオラクル Sensing が与えられたとき，$\mathbb{X}_T$ に含まれる物体に対する電子署名を考えるものとする．まず述語関数 $R$ を定義 4.8 の Relation Function とする．また，定義 4.2 より物体集合 $\mathbb{X}_T$ に属する物体に対して与えられた Sensing は次の性質を満たす：

$$\begin{gathered}\text{for all } x_i, x_j \in \mathbb{X}_T \text{ s.t. } \mathsf{isSame}(\boxed{x_i}, \boxed{x_j}) = 0, \\ \text{if } D_i \leftarrow \mathsf{Sensing}(\boxed{x_i}) \text{ and } D_j \leftarrow \mathsf{Sensing}(\boxed{x_j}), \\ \text{then we have } \Pr[D_i = D_j] = 0\end{gathered}$$

提案方式 $\Pi_1 = (\mathsf{SfO.KG}, \mathsf{SfO.Sign}, \mathsf{SfO.Ver})$ は以下のようになる：

- $\mathsf{SfO.KG}(1^\lambda)$：$\mathsf{DS.KG}(1^\lambda) \to (pk, sk)$ を出力する．
- $\mathsf{SfO.Sign}(sk, \boxed{x})$：電子データ $D \leftarrow \mathsf{Sensing}(\boxed{x})$ を得る．$\hat{\sigma} \leftarrow \mathsf{DS.Sign}(sk, D)$ を計算し，署名 $\sigma = (D, \hat{\sigma})$ を出力する．
- $\mathsf{SfO.Ver}(pk, \boxed{x}, \sigma)$：電子データ $D' \leftarrow \mathsf{Sensing}(\boxed{x})$ を得て $\mathsf{DS.Ver}(pk, D, \hat{\sigma}) \wedge R(D, D')$ を出力する．

**正当性．** ある $\lambda$, $T$, $x \in \mathbb{X}_T$ について $(pk, sk) \leftarrow \mathsf{SfO.KG}(1^\lambda)$ および $\sigma = (D, \hat{\sigma}) \leftarrow \mathsf{SfO.Sign}(sk, \boxed{x})$ とする．このとき，電子署名方式 $\Sigma_{DS}$ の正当性から常に $\mathsf{DS.Ver}(pk, D, \hat{\sigma}) = 1$ が成立する．また，センシングの性質より，同じ物体から得た異なるセンシングデータ $D, D'$ は常に $R(D, D') = 1$ となるので，提案方式 $\Pi_1$ は正当性を満たす．

**定理 5.1.** 通常の電子署名方式 $\Sigma_S$ が $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA 攻撃者に対して定義 4.5 の EUF-CMA 安全性を満たすならば，上の提案方式 $\Pi_1$ も $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA 攻撃者に対して定義 5.1 の EUF-COA を満たす．

**証明.** $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA を実行可能な攻撃者 $A$ を提案方式 $\Pi_1$ に対する攻撃者とし，その攻撃成功確率を $\mathrm{Succ}_A^O$ とする．この $A$ を用いて従来の署名方式に対する攻撃者 $B$ を構成する．ただし $B$ も $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA を実行可能なものとする．$B$ の攻撃成功確率 $\mathrm{Succ}_B^S$ は次のように定義できる：

$$\mathrm{Succ}_B^S = \Pr\left[\begin{array}{c}(pk, sk) \leftarrow \mathsf{KG}(\lambda); \\ (m, \sigma) \leftarrow B^{\mathsf{DS.Sign}(sk, \cdot)}(pk) : \\ \mathsf{DS.Ver}(pk, m, \sigma) = 1 \wedge m \notin \mathcal{M}\end{array}\right]$$

ただし $\mathcal{M}$ は $B$ がオラクル $\mathsf{DS.Sign}(sk, \cdot)$ にクエリするメッセージの集合である．
$B$ は以下のように記述できる（ただし，ラベル $l_x$ は物体 $x$ を指し示し，ラベル $l_{x_A}$ は物体 $x_A$ を指し示す）：

$B(pk)$
　run $A(pk)$
　　when $A$ queries $l_x$ to $\mathsf{Adv.Command}(\cdot)$
　　(i.e. $A$ does $\mathsf{Command} \in \mathbb{C}$ to $x \in \mathbb{X}_A$),
　　query $\mathsf{Adv.Command}(l_x)$ and receive $\epsilon$
　　(add the new object to $\mathbb{X}_A$)
　　when $A$ queries $l_x$ to $\mathsf{Adv.Sensing}(\cdot)$
　　(i.e. $A$ asks a sensing data for $x \in \mathbb{X}_A$),
　　query $\mathsf{Adv.Sensing}(l_x)$ and receive $D$
　　return $D$ to $A$
　　when $A$ queries $l_{x_i}$ to $\mathsf{Adv.Sign}(sk, \cdot)$

(i.e. $A$ asks a signature for $x_i \in \mathbb{X}_A$),
query $\mathsf{Adv.Sensing}(l_{x_i})$ and receive $D_i$
add $D_i$ to $\mathcal{D}$
query $D_i$ to $\mathsf{DS.Sign}(sk, \cdot)$ and receive $\hat{\sigma}_i$
return $\sigma_i = (D_i, \hat{\sigma}_i)$ to $A$
$A$ outputs $(l_{x_A}, \sigma_A = (D_A, \hat{\sigma}_A))$
if $D_A \notin \mathcal{D}$, then return $(D_A, \hat{\sigma}_A)$;
otherwise, abort

上のアルゴリズム $B$ は内部で $A$ のシミュレーションを行っている．$A$ の出力が正しければその定義より必ず $\mathsf{DS.Ver}(pk, D_A, \hat{\sigma}_A) = 1$ および $D'_A \leftarrow \mathsf{Sensing}(\boxed{x_A})$ に対して $R(D'_A, D_A) = 1$ と $R(D'_A, D_i) = 0$ for all $D_i \in \mathcal{D}$ が成立する．

ここで，$D_A \notin \mathcal{D}$ となる確率について考える．各 $D_i \in \mathcal{D}$ に対して，$R(D'_A, D_A) = 1$ かつ $R(D'_A, D_i) = 0$ より，センシングにより $D_A$ を得た物体と $D_i$ を得た物体は異なる物体である．センシングが満たす性質より，異なる物体のセンシングデータは異なるため，常に $\Pr[D_A = D_i] = 0$ となる．以上より，

$$\mathrm{Succ}_A^O \leq \mathrm{Succ}_B^S \leq negl(\lambda)$$

□

# Chapter 6　モノの秘匿性の安全性定義とその構成

## 6.1　本章の概要

この章では，モノの電子署名特有の課題を解決するために導入した新たな安全性であるモノの秘匿性を説明する．モノの電子署名特有の課題とは，署名から物体の情報が漏洩してしまう場合に署名を手に入れた悪意のある人がその署名を用いた物体の偽造を行う可能性が存在することであった．ゆえに，署名単体からは物体の情報が漏れないという性質をモノの秘匿性として安全性定義を行う．また，EUF-COA 安全性とモノの秘匿性の両方を満たす証明可能安全な構成も示す．これは，物体のセンシングデータの確率的ハッシュを取りそのハッシュ値に対して署名を行う，という構成である．基盤とする電子署名方式が PEA 攻撃者に対して EUF-CMA 安全であり，確率的ハッシュが弱衝突困難性を満たすならば，モノの電子署名方式は EUF-COA 安全性を満たし，PEA 攻撃者に対して Relational Hash が $\lambda$-source に関する偽造不可能性を満たすならば，モノの電子署名方式はモノの秘匿性を満たすことを示す．

7 章にて，この仮定を満たす Relational Hash の構成を示すが，現時点では原像の組の関係としてハミング距離が一定値以下であるような関係の Relational Hash の構成しか見つけられていない（すなわち，関係 $R_\delta = \{dist(x, y) \leq \delta\}$ に関する Relational Hash）．したがって，定義 4.2 に加えてセンシングは次の 2 つの性質を満たすものとする：

- ある物体 $x \in \mathbb{X}$ について
  $D_x \leftarrow \mathsf{Sensing}(\boxed{x})$, $D'_x \leftarrow \mathsf{Sensing}(\boxed{x})$ とすると $dist(D_x, D'_x) \leq \delta$ を満たす．
- 異なる 2 つの物体 $x, y \in \mathbb{X}$（すなわち $\mathsf{isSame}(\boxed{x}, \boxed{y}) = 0$） について
  $D_x \leftarrow \mathsf{Sensing}(\boxed{x})$, $D_y \leftarrow \mathsf{Sensing}(\boxed{y})$ とすると $dist(D_x, D_y) > \delta$ を満たす．

## 6.2　モノの秘匿性の安全性定義

モノの電子署名方式の新たな安全性定義としてモノの秘匿性を定義する．これは簡単にいうと，物体空間が十分なエントロピーを持つ限り署名から対応する物体を特定することが困難である，という安全性を表す．

攻撃者は初期状態として，物体集合 $\mathbb{X}_T$ およびそのラベル集合 $L_\mathbb{X}$，コマンドオラクルの集合 $\mathbb{C}$，センシングオラクル $\mathsf{Sensing}$ をもっている．ここから攻撃者はセキュリティパラメータの多項式サイズの回路で表現できるラベルの分布 $\mathcal{L}_\mathbb{X}$ を作成し，それを挑戦者に送る．挑戦者は受け取ったラベルの分布に従い，ランダムにラベル $l_x$ を 1 つサンプルする．そのラベルが指し示す物体 $x$ について $\mathsf{SfO.Sign}(sk, \boxed{x})$ を実行し署名 $\sigma$ を得ると，それを攻撃者に送る．署名 $\sigma$ を受け取った攻撃者は次の 3 つのオラクルに任意

の回数ラベルをクエリできる：Adv.Sign$(sk,\cdot)$，Adv.Sensing$(\cdot)$，Adv.Command$(\cdot)$．これらのオラクルは物体 $x$ のラベルが $l_x$ を受け取るとそれぞれ，Adv.Sign$(sk, l_x)$ は物体 $x$ の署名を返し，Adv.Sensing$(l_x)$ は物体 $x$ のセンシングデータを返し，Adv.Command$(l_x)$ は物体 $x$ に対して対応するコマンドを実行する．その後，攻撃者は物体のラベル $l_{x_A}$ を出力する．このとき，SfO.Ver$(pk, \boxed{x_A}, \sigma) = 1$ を攻撃者の勝利条件とし，攻撃者が勝利する確率が十分に小さいとき，そのモノの電子署名方式はモノの秘匿性を満たす，とする．

これをゲームとして記述すると以下のようになる：

***Setup.*** あらかじめ物体集合 $\mathbb{X}_T$ とそのラベル集合 $L_{\mathbb{X}}$，コマンドオラクル集合 $\mathbb{C}$，センシングオラクル Sensing は与えられているものとする．はじめに挑戦者は鍵生成アルゴリズム SfO.KG$(1^\lambda)$ を実行して鍵 $(pk, sk)$ を作成し，検証鍵 $pk$ を攻撃者に渡す．ただし，$\mathbb{X}_T$ は方式構成時に与えられる物体集合 $\mathbb{X}_m$ に Command $\in \mathbb{C}$ を $T$ 回実行して得られる物体全てを含む集合である．

***Action1.*** 攻撃者 $A_1$ はラベル集合 $L_{\mathbb{X}}$ 上の分布 $\mathcal{L}_{\mathbb{X}}$ を作成し，それを挑戦者に送る．挑戦者は受け取ったラベルの分布から 1 つラベル $l_{x^*}$ をサンプルし，その物体の署名 $\sigma^* \leftarrow$ SfO.Sign$(sk, \boxed{x^*})$ を攻撃者に送る．

***Action2.*** 攻撃者 $A_2$ は以下の 3 つの動作を実行できる．(i) 1 つは，物体 $x \in \mathbb{X}_T$ に任意のコマンド Command $\in \mathbb{C}$ を実行して新たな物体を作成する，という動作である．攻撃者は作成した物体にラベルを付与し，物体を集合 $\mathbb{X}_T$ に加える．コマンド実行ごとに新規物体のラベル情報は挑戦者に共有される．(ii) 1 つは，オラクル Adv.Sensing$(\cdot)$ にラベル $l_x$ をクエリして物体 $x \in \mathbb{X}_T$ の電子データを得る，という動作である．(iii) 1 つは，オラクル Adv.Sign$(sk,\cdot)$ にラベル $l_x$ をクエリして物体 $x \in \mathbb{X}_T$ の署名を得る，という動作である．

***Forgery.*** 攻撃者 $A$ は物体 $x_A$ を指し示すラベル $l_{x_A}$ を出力する．

$A = (A_1, A_2)$ の勝利条件は $l_{x_A}$ について以下の式が成立することとする：

$$dist(D^*, D_A) \leq \delta$$
$$\text{where } D^* \leftarrow \text{Sensing}(\boxed{x^*}) \text{ and } D_A \leftarrow \text{Sensing}(\boxed{x_A})$$

**定義 6.1.** 上に記述したゲームにおける攻撃者 $A$ の攻撃成功確率を $\mathrm{Succ}_A^{OP}$ とする．モノの電子署名方式 $\Pi =$ (SfO.KG,SfO.Sign, SfO.Ver) が $(\mathbb{X}_T, \mathbb{C}, \text{Sensing})$ でパラメタライズされた任意の PEA 攻撃者 $A$ に対してモノの秘匿性を満たすとは $\mathrm{Succ}_A^{OP}$ が無視できる確率であることである．すなわち $\mathrm{Succ}_A^{OP} \leq negl(\lambda)$ であれば，その方式は $(\mathbb{X}_T, \mathbb{C}, \text{Sensing})$ でパラメタライズされた PEA 攻撃者に対してモノの秘匿性を満たす．

## 6.3　EUF-COA とモノの秘匿性を満たす構成

EUF-COA とモノの秘匿性を満たすモノの電子署名方式を，通常の電子署名と Relational Hash を組み合わせることで構成し，その安全性証明を行う．通常の電子署名方式

を $\Sigma_{DS} = (\mathsf{DS.KG}, \mathsf{DS.Sign}, \mathsf{DS.Ver})$，関係 $R_\delta = \{(x, y, \delta) \mid dist(x, y) \leq \delta\} \subseteq X \times Y \times Z$ の Relational Hash 方式を $\Sigma_{RH} = (\mathsf{RH.KG}, H_R, H'_R, \mathsf{RH.Ver})$ とする（すなわち，常に $z = \delta$ であるような Relational Hash）．物体集合 $\mathbb{X}_m$，コマンドオラクル集合 $\mathbb{C}$，センシングオラクル Sensing が与えられたとき，$\mathbb{X}_T$ に含まれる物体に対する電子署名を考えるものとする．

提案方式 $\Pi_2 = (\mathsf{SfO.KG}, \mathsf{SfO.Sign}, \mathsf{SfO.Ver})$ は以下のようになる：

- $\mathsf{SfO.KG}(1^\lambda)$：$(pk_{DS}, sk_{DS}) \leftarrow \mathsf{DS.KG}(1^\lambda)$ および
  $pk_{RH} \leftarrow \mathsf{RH.KG}(1^\lambda)$ を計算し $pk := (pk_{DS}, pk_{RH})$, $sk := (sk_{DS}, pk_{RH})$ を出力する．

- $\mathsf{SfO.Sign}(sk, \boxed{x})$：電子データ $D \leftarrow \mathsf{Sensing}(\boxed{x})$ を得る．$\sigma_1 \leftarrow H_R(pk_{RH}, D)$ および
  $\sigma_2 \leftarrow \mathsf{DS.Sign}(sk_{DS}, \sigma_1)$ を計算し，署名 $\sigma = (\sigma_1, \sigma_2)$ を出力する．

- $\mathsf{SfO.Ver}(pk, \boxed{x}, \sigma)$：電子データ $D' \leftarrow \mathsf{Sensing}(\boxed{x})$ を得る．また $\sigma$ を $(\sigma_1, \sigma_2)$ にパースする．まず
  $\mathsf{DS.Ver}(pk_{DS}, \sigma_1, \sigma_2) = 0$ であれば $0$ を出力する．そうでないならば $\mathsf{RH.Ver}(pk_{RH}, \sigma_1, H'_R(pk_{RH}, D'), \delta)$ を出力する．

詳細は 7.4 節に記すが，構成要素である関係 $R_\delta$ の Relational Hash 方式 $\Sigma_{RH} = (\mathsf{RH.KG}, H_R, H'_R, \mathsf{RH.Ver})$ について，確率的ハッシュ $H_R, H'_R$ は定義 3.3 の衝突困難性を満たすことができない．そこで，確率的ハッシュの弱衝突困難性を定義する．

**定義 6.2.** 鍵空間 $\{K_\lambda\}$，乱数空間 $\{R_\lambda\}$ の確率的関数族 $H^{(\lambda)} = \{h_k\}_{k \in K_\lambda}$ について，どのような PPTA 攻撃者 $A$ に対しても次の式が成立するような無視可能関数 $negl(\lambda)$ が存在するとき，$H^{(\lambda)}$ は弱衝突困難性を満たすという．

$$\Pr\left[\begin{array}{l} k \leftarrow K_\lambda; (x, y, r, s) \leftarrow A(k) : \\ \quad x \neq y \wedge h_k(x, r) = h_k(y, s) \end{array}\right] < negl(\lambda) \tag{6.1}$$

ただし，$r, s \in R_\lambda$ とする．

4.3 節と同様に，本稿で提案する方式には PEA 攻撃者に対して弱衝突困難性を満たす確率的ハッシュが必要であるため，以下で定義する．

**定義 6.3.** 定義 6.2 では PPTA 攻撃者に対する安全性を定義したが，$(\mathbb{X}_T, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA 攻撃者 $A$ に対しても同様に安全性を定義できる．どんな PEA 攻撃者 $A$ に対しても式 (6.1) が成立するような無視可能関数 $negl()$ が存在するとき，確率的ハッシュは PEA 攻撃者に対して弱衝突困難性を満たすという．

**正当性**　ある $\lambda$, $T$, $x \in \mathbb{X}_T$ について $(pk, sk) \leftarrow \mathsf{SfO.KG}(1^\lambda)$ および $\sigma = (\sigma_1, \sigma_2) \leftarrow \mathsf{SfO.Sign}(sk, \boxed{x})$ とする．このとき，電子署名方式 $\Sigma_{DS}$ の正当性から常に $\mathsf{DS.Ver}(pk, \sigma_1, \sigma_2) = 1$ が成立する．また，センシングの性質より同じ物体から得た異なるセンシングデータ $D, D'$ は $dist(D, D') \leq \delta$ となるので，関係 $R_\delta$ の Relational Hash 方式 $\Sigma_{RH}$ の正当性から $\mathsf{RH.Ver}(pk_{RH}, \sigma_1, H'_R(pk_{RH}, D'), \delta) = 1$ となる．ゆえに提案方式 $\Pi_2$ は正当性を満たす.

**定理 6.1.** 通常の電子署名方式 $\Sigma_S$ が $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA 攻撃者に対して定義 4.5 の EUF-CMA 安全性を満たし，かつ確率的ハッシュ関数 $H_R$ が定義 4.6 の衝突困難性を満たすならば，上の提案方式 $\Pi_2$ は $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA 攻撃者に対して定義 5.1 の EUF-COA を満たす.

**証明.** $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA を実行可能な攻撃者 $A$ を提案方式 $\Pi_2$ の EUF-COA に対する攻撃者とし，その攻撃成功確率を $\mathrm{Succ}^O_A$ とする．この $A$ を用いて従来の署名方式の EUF-CMA に対する攻撃者 $B$ を構成する．ただし $B$ も $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA を実行可能なものとする．$B$ の攻撃成功確率 $\mathrm{Succ}^{DS}_B$ は次のように定義できる：

$$\mathrm{Succ}^{DS}_B = \Pr\left[\begin{array}{c}(pk_{DS}, sk_{DS}) \leftarrow \mathsf{DS.KG}(1^\lambda); \\ (m, \sigma) \leftarrow B^{\mathsf{DS.Sign}(sk_{DS}, \cdot)}(pk_{DS}) : \\ \mathsf{DS.Ver}(pk_{DS}, m, \sigma) = 1 \wedge m \notin \mathcal{M}\end{array}\right]$$

ただし $\mathcal{M}$ は $B$ がオラクル $\mathsf{DS.Sign}(sk_{DS}, \cdot)$ にクエリするメッセージの集合である．$B$ は以下のように記述できる（ただし，ラベル $l_x$ は物体 $x$ を指し示し，ラベル $l_{x_A}$ は物体 $x_A$ を指し示す）：

$B(pk_{DS})$
　run $pk_{RH} \leftarrow \mathsf{RH.KG}(1^\lambda)$
　let $pk := (pk_{DS}, pk_{RH})$
　let $\mathcal{D} = Sig = \emptyset$
　run $A(pk)$
　　when $A$ queries $\mathsf{Adv.Command}(l_x)$
　　(i.e. $A$ does $\mathsf{Command} \in \mathbb{C}$ to $x \in \mathbb{X}_A$),
　　query $\mathsf{Adv.Command}(l_x)$ and receive $\epsilon$
　　(add the new object to $\mathbb{X}_A$)
　　when $A$ queries $\mathsf{Adv.Sensing}(l_x)$
　　(i.e. $A$ asks a sensing data for $x \in \mathbb{X}_A$),
　　query $\mathsf{Adv.Sensing}(l_x)$ and receive $D$
　　return $D$ to $A$
　　when $A$ queries to $\mathsf{Adv.Sign}(sk, l_{x_i})$
　　(i.e. $A$ asks a signature for $x_i \in \mathbb{X}_A$),
　　query $\mathsf{Adv.Sensing}(l_{x_i})$ and receive $D_i$

add $D_i$ to $\mathcal{D}$
compute $\sigma_{i,1} \leftarrow H_R(pk_{RH}, D_i)$
add $\sigma_{i,1}$ to $Sig$
query $\mathsf{DS.Sign}(sk_{DS}, \sigma_{i,1})$ and receive $\sigma_{i,2}$
return $\sigma_i = (\sigma_{i,1}, \sigma_{i,2})$ to $A$
$A$ outputs $(l_{x_A}, \sigma_A = (\sigma_{A,1}, \sigma_{A,2}))$
if $\sigma_{A,1} \notin Sig$, then return $(\sigma_{A,1}, \sigma_{A,2})$;
otherwise, abort

上のアルゴリズム $B$ は内部で $A$ のシミュレーションを行っている．$A$ の出力が正しければその定義より必ず $\mathsf{DS.Ver}(pk_{DS}, \sigma_{A,1}, \sigma_{A,2}) = 1$ と $D_B \leftarrow \mathsf{Sensing}(\boxed{x_A})$ に対して $\mathsf{RH.Ver}(pk_{RH}, \sigma_{A,1}, H'_R(pk_{RH}, D_B)) = 1$ と $dist(D_A, D_i) > \delta$ for all $D_i \in \mathcal{D}$ が成立する．

ここで，$\sigma_{A,1} \notin Sig$ となる確率について考える．各 $D_i \in \mathcal{D}$ に対して $dist(D_A, D_i) > \delta$ より常に $D_A \neq D_i$．すなわち，ある $\sigma_{i,1} \in Sig$ に対して $\sigma_{A,1} = \sigma_{i,1}$ となるのは，$D_A \neq D_i$ となる $i$ に対して $H_R(pk_{RH}, D_A) = H_R(pk_{RH}, D_i)$ となるときのみである．ここで $D_i$ を与えられたとき $H_R(pk_{RH}, D_A, r) = H_R(pk_{RH}, D_i, s)$ となる $D_A$ を無視可能でない確率で見つけるアルゴリズム $C$ が存在したとする．ただし，乱数 $r, s$ は攻撃者が選ぶことができることに注意が必要である．これを用いて $H_R$ の弱衝突困難性に対する攻撃者 $D$ を構成する．$D$ はまず $H_R$ への入力として $D_i$ を選び，$C$ にクエリする．$C$ は $H_R(pk_{RH}, D_A, r) = H_R(pk_{RH}, D_i, s)$ となる $D_A$ および計算に用いた乱数 $r, s$ の情報を $D$ に返す．このとき，$D$ が $(D_A, D_i, r, s)$ を出力すると それは $H_R$ の弱衝突困難性を破る．これはタイトな帰着であり，また仮定より，どの PEA 攻撃者も $H_R$ の弱衝突困難性を破る確率は高々 $negl(\lambda)$ であるため，$\sigma_{A,1} = \sigma_{i,1}$ となる確率も高々 $negl(\lambda)$ である．Union Bound より $\Pr[\sigma_{A,1} \in Sig] \leq \sum_i \Pr[\sigma_{A,1} = \sigma_{i,1}]$ であるから，

$$\begin{aligned} \mathrm{Succ}_B^{DS} &\geq \mathrm{Succ}_A^{O} - \Pr[\sigma_{A,1} \in Sig] \\ &\geq \mathrm{Succ}_A^{O} - \sum_i \Pr[\sigma_{A,1} = \sigma_{i,1}] \\ &\geq \mathrm{Succ}_A^{O} - |Sig| \cdot negl(\lambda) \end{aligned}$$

$|Sig| \leq poly(\lambda)$ であるから，上の式より，

$$\mathrm{Succ}_A^{O} \leq \mathrm{Succ}_B^{DS} + negl(\lambda) \leq negl(\lambda)$$

□

**定理 6.2.** 関係 $R_\delta$ の Relational Hash 方式 $\Sigma_{RH}$ が $(\mathbb{X}_T, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA 攻撃者に対して定義 4.7 の偽造不可能性を満たすならば，提案方式 $\Pi_2$ は $(\mathbb{X}_T, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた $\lambda$-source PEA 攻撃者に対して定義 6.1 のモノの秘匿性を満たす．

**証明.** $(\mathbb{X}_T, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA を実行可能な攻撃者 $A = (A_1, A_2)$ を提案方式 $\Pi_2$ のモノの秘匿性に対する攻撃者とし，その攻撃成功確率を $\mathrm{Succ}_A^{OP}$ とする．この $A$ を用いて関係 $R_\delta \subseteq X \times Y \times Z$ の Relational Hash の $X$ 上の $\lambda$-source 分布 $\mathcal{X}$ に関する偽造不可能性に対する攻撃者 $B$ を構成する．ただし $B$ も $(\mathbb{X}_T, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA を実行可能なものとする．$B$ の攻撃成功確率 $\mathrm{Succ}_B^{UF}$ は次のように定義できる：

$$\mathrm{Succ}_B^{UF} = \Pr\left[\begin{array}{c} pk_{RH} \leftarrow \mathsf{RH.KG}(1^\lambda); \\ x \leftarrow \mathcal{X}; hx \leftarrow H_R(pk_{RH}, x); \\ hy' \leftarrow B(pk_{RH}, hx) : \\ \mathsf{RH.Ver}(pk_{RH}, hx, hy', \delta) = 1 \end{array}\right]$$

まず定義 6.1 のゲームにおける *Action1.* を考える．$A_1$ の実行により，ラベル集合 $L_{\mathbb{X}_T}$ 上のある分布 $\mathcal{L}_{\mathbb{X}_T}$ が出力されたとする．このとき $A$ は $\lambda$-source 攻撃者であるから，全ての物体のセンシングデータの分布を $\mathcal{D}_{\mathbb{X}_T}$ とすると，常に $H_\infty(\mathcal{D}_{\mathbb{X}_T}) \geq \lambda$ が成立する．$B$ に対する挑戦者は分布 $\mathcal{L}_{\mathbb{X}}$ からランダムにラベル $l_{x^*}$ をサンプルし，対応する物体 $x^*$ のセンシングデータ $D^* \leftarrow \mathsf{Sensing}(\boxed{x^*})$ を得た後，$h_{D^*} \leftarrow H_R(pk_{RH}, D^*)$ を計算する．

この状況の下で $B$ は以下のように記述できる：

$B(pk_{RH}, h_{D^*})$
  run $\mathsf{DS.KG}(1^\lambda) \rightarrow (pk_{DS}, sk_{DS})$
  let $pk := (pk_{DS}, pk_{RH})$
  compute $\hat{\sigma} \leftarrow \mathsf{DS.Sign}(sk_{DS}, h_{D^*})$
  let $\sigma^* := (h_{D^*}, \hat{\sigma})$
  run $A_2(pk, \sigma^*)$
    when $A_2$ queries $\mathsf{Adv.Command}(l_x)$
     (i.e. $A_2$ does $\mathsf{Command} \in \mathbb{C}$ to $x \in \mathbb{X}_A$),
       query $\mathsf{Adv.Command}(l_x)$ and receive $\epsilon$
       (add the new object to $\mathbb{X}_A$)
    when $A_2$ queries $\mathsf{Adv.Sensing}(l_x)$
     (i.e. $A_2$ asks a sensing data for $x \in \mathbb{X}_A$),
       query $\mathsf{Adv.Sensing}(l_x)$ and receive $D$
       return $D$ to $A_2$
    when $A_2$ queries to $\mathsf{Adv.Sign}(sk, l_{x_i})$
     (i.e. $A_2$ asks a signature for $x_i \in \mathbb{X}_A$),
       query $\mathsf{Adv.Sensing}(l_{x_i})$ and receive $D_i$
       compute $\sigma_{i,1} \leftarrow H_R(pk_{RH}, D_i)$
       compute $\sigma_{i,2} \leftarrow \mathsf{DS.Sign}(sk_{DS}, \sigma_{i,1})$
       return $\sigma_i = (\sigma_{i,1}, \sigma_{i,2})$ to $A_2$
  $A_2$ outputs $l_{x_A}$
  compute $D_A \leftarrow \mathsf{Sensing}(\boxed{x_A})$

output $h_{D_A} \leftarrow H'_R(pk_{RH}, D_A)$

$B$ は内部で定義 6.1 のゲームにおける *Action2.* である $A_2$ のシミュレーションを行っている．$A_2$ の出力が正しければ必ず $dist(D^*, D_A) \leq \delta$ となるため，$\mathsf{RH.Ver}(pk_{RH}, h_{D^*}, h_{D_A}, \delta) = 1$ が成立する．すなわち $\lambda$-source となる分布に対して $B$ は常に攻撃が成功する．ゆえに，

$$\mathrm{Succ}_A^{OP} \leq \mathrm{Succ}_B^{UF} \leq negl(\lambda)$$

□

# Chapter 7　安全性証明の仮定に関する考察

## 7.1　本章の概要

これまでは 1 章で説明した一般的構成法の考えに則り，構成の基盤として既存の方式を用いた．この章では，安全性証明の帰着に用いられた方式の安全性を満たす構成について，より具体的に議論する．本稿で証明した安全性に必要な仮定は以下の三つである：(1) 定義 4.5 で示した PEA 攻撃者に対して EUF-CMA 安全な電子署名方式 (2) 定義 4.7 で示した PEA 攻撃者に対して $\lambda$-source に関する偽造不可能性を満たす Relational Hash (3) 定義 6.3 で示した PEA 攻撃者に対して弱衝突困難性を満たす確率的ハッシュ．(1) の議論の中で PPTA 攻撃者に対して安全な方式が果たして PEA 攻撃者に対して安全であるのか論じる．詳細は次節に示すが，本稿では PPTA 攻撃者に対して安全であるならば PEA 攻撃者に対して安全であるものと仮定する．ゆえに，(2) および (3) の構成を示す際には PPTA 攻撃者に対する安全性を証明する．

## 7.2　PEA 攻撃者に対して EUF-CMA 安全な電子署名方式

定義 3.2 で示した通り，従来の電子署名方式の安全性では攻撃者の攻撃能力として PPTA を考えている（耐量子仮定を考える場合は除く）．それを今回必要であるからという理由で定義 4.5 を導入し，定理 5.1 や定理 6.1 および定理 6.2 でそれを仮定している．しかし，定義 3.2 の安全性を満たす電子署名方式は定義 4.5 の安全性を満たすのかどうかは議論が必要である．

直観的には，PPTA 攻撃者に対して安全であれば PEA 攻撃者に対して安全であるように思える．なぜなら，どんな PPTA でも破れない安全性が物理空間で多項式時間以内に得られる情報により破られるとは考えにくいからである．しかし，注意が必要なのは，本稿の定式化では物理空間での操作をオラクルで表現しておりオラクルへクエリすることで物理的な操作を行う，つまり，物体を生成するのに必要な時間はほとんど考慮しておらず，単に生成回数が多項式回であればその方式は全体として多項式時間で実行される，ということである．オラクルへの多項式回のクエリで生成できる物体に，たとえば素因数分解を解くことができるハードウェアが含まれているならば PPTA に対して安全な方式が常に PEA に対して安全とは言えなくなる．これは数学的な解析が及ぶ部分ではなく，そういった PPTA では解くことができなかった問題が解けるようなハードウェアは多項式時間で生成できないものという仮定をおくことが限度である．ゆえに以下の仮定をおく．

**仮定 7.1.** ある問題 $P$ はどんな PPTA でも解くことが困難であるものとする．このとき，物体集合 $\mathbb{X}_m$ に PPTA で解くことができない問題を解ける物体が含まれていなければ，どんなコマンドオラクル集合 $\mathbb{C}$，センシングオラクル Sensing に対しても $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA は常に多項式時間で問題 $P$ を解くことが困難である．

まとめとして，本稿では PPTA 攻撃者に対して安全な方式は全て PEA 攻撃者に対して安全であるという仮定のもと議論を進める．次節以降，Relational Hash や確率的ハッシュの安全性に関して構成の提案とその安全性証明を行うがこれは PPTA 攻撃者に対してであり，定義 4.7 や定義 6.3 を満たす構成を直接示すわけではないが，本稿に限り上の議論から十分であるとする．

## 7.3　$\lambda$-source に関する偽造不可能性を満たす Relational Hash

ここでは，関係 $R_\delta = \{dist(x,y) \leq \delta\} \subseteq X \times Y \times Z$ の Relational Hash が $\lambda$-source に関する偽造不可能性を満たす構成を示す．構成には関係 $R_{lin} = \{x+y=z \wedge x,y,z \in \mathbb{F}_2^k\}$ の Relational Hash (以下 linear Relational Hash) と $(n,k,d)$ linear ECC を組み合わせる．そこで (i) $\lambda$-source に関する偽造不可能性を満たす linear Relational Hash の構成を示し (ii) linear Relational Hash が $\lambda$-source に関する偽造不可能性を満たすならば上の構成も $\lambda$-source に関する偽造不可能性を満たすことを示す．

### (i) $\lambda$-source に関する偽造不可能性を満たす linear Relational Hash

定義域 $X,Y,Z = \mathbb{F}_2^k$ に対して関係 $R_{lin} = \{(x,y,z) \mid x+y=z \wedge x,y,z \in \mathbb{F}_2^k\}$ の Relational Hash の構成 $\Pi_{R_{lin}} = (\mathsf{RH}_{lin}.\mathsf{KG}, H_{R_{lin}}, H'_{R_{lin}}, \mathsf{RH}_{lin}.\mathsf{Ver})$ は以下のようになる：

$\mathsf{RH}_{lin}.\mathsf{KG}(1^\lambda)$：$q$ をセキュリティパラメータ $\lambda$ の指数サイズの素数とする．また，$\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ を位数 $q$ の巡回群とし，写像 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ を双線形写像とする．まず，二つの生成元 $\boldsymbol{g}_0 \leftarrow \mathbb{G}_1, \boldsymbol{h}_0 \leftarrow \mathbb{G}_2$ を得る．次に，$\langle a_i \rangle_{i=1}^{k+1}, \langle b_i \rangle_{i=1}^{k+1}$ を全て $\mathbb{Z}_q^*$ からランダムに選ぶ．$\boldsymbol{g}_i := \boldsymbol{g}_0^{a_i}, \boldsymbol{h}_i := \boldsymbol{h}_0^{b_i}$ とし，以下で定義される $pk := (pk_1, pk_2, pk_R)$ を出力する：

$$pk_1 := \langle \boldsymbol{g}_i \rangle_{i=0}^{k+1}, \quad pk_2 := \langle \boldsymbol{h}_i \rangle_{i=0}^{k+1}, \quad pk_R := \sum_{i=1}^{k+1} a_i b_i$$

$H_{R_{lin}}(pk, x)$: $pk$ と $x = \langle x_i \rangle_{i=1}^k \in \mathbb{F}_2^k$ を入力として受け取る．ランダムに $r \in \mathbb{Z}_q^*$ をサンプルし以下で計算される $hx$ を出力する：

$$hx := \left( \boldsymbol{g}_0^r, \left\langle \boldsymbol{g}_i^{(-1)^{x_i} r} \right\rangle_{i=1}^k, \boldsymbol{g}_{k+1}^r \right)$$

$H'_{R_{lin}}(pk, y)$: $pk$ と $y = \langle y_i \rangle_{i=1}^{k} \in \mathbb{F}_2^k$ を入力として受け取る．ランダムに $s \in \mathbb{Z}_q^*$ をサンプルし以下で計算される $hy$ を出力する：

$$hy := \left( \boldsymbol{h}_0^s, \left\langle \boldsymbol{h}_i^{(-1)^{y_i} s} \right\rangle_{i=1}^{k}, \boldsymbol{h}_{k+1}^s \right)$$

$\mathsf{RH}_{lin}.\mathsf{Ver}(pk, hx, hy, z)$: $pk, hx = \langle hx_i \rangle_{i=0}^{n+1}, hy = \langle hy_i \rangle_{i=0}^{n+1}, z = \langle z_i \rangle_{i=1}^{n} \in \mathbb{F}_2^n$ を入力として受け取り，次の等号が成立するかどうか検証する：

$$e\left(hx_0, hy_0\right)^{pk_R} \stackrel{?}{=} e\left(hx_{k+1}, hy_{k+1}\right) \prod_{i=1}^{k} e\left(hx_i, hy_i\right)^{(-1)^{z_i}}$$

$x + y = z$ とすると

$$\begin{aligned} e\left(hx_{k+1}, hy_{k+1}\right) \prod_{i=1}^{k} e\left(hx_i, hy_i\right)^{(-1)^{z_i}} &= e\left(g_0, g_0\right)^{a_{k+1} b_{k+1} rs} \prod_{i=1}^{k} e\left(g_0, g_0\right)^{a_i b_i (-1)^{x_i} (-1)^{y_i} rs (-1)^{z_i}} \\ &= \prod_{i=1}^{k+1} e\left(hx_0, hy_0\right)^{a_i b_i} \\ &= e\left(hx_0, hy_0\right)^{pk_R} \end{aligned}$$

ゆえにこの方式は正当性を満たす.

以上の構成に関して次の定理を示したい.

**定理 7.1.** 上で示した構成 $\Pi_{R_{lin}} = (\mathsf{RH}_{lin}.\mathsf{KG}, H_{R_{lin}}, H'_{R_{lin}}, \mathsf{RH}_{lin}.\mathsf{Ver})$ は，確率分布 $\mathcal{X}$ を $\lambda$-source としたとき，定義 3.6 で示した確率分布 $\mathcal{X}$ に関する偽造不可能性を満たす.

**証明.** 証明は次の三つのパートからなる：

1. 関係 $R_{lin}$ が $\lambda$-source である分布 $\mathcal{X}, \mathcal{Y}$ に関して sparse relation となることを示す.

2. 二つの確率的ハッシュ $H_{R_{lin}}, H'_{R_{lin}}$ がそれぞれ，$\lambda$-source である分布 $\mathcal{X}, \mathcal{Y}$ と鍵生成アルゴリズム $\mathsf{RH}_{lin}.\mathsf{KG}$ の出力分布 $\mathcal{K}$ に関して定義 3.4 の 2-POW を満たすことを示す.

3. $(\mathsf{RH}_{lin}.\mathsf{KG}, H_{R_{lin}}, H'_{R_{lin}}, \mathsf{RH}_{lin}.\mathsf{Ver})$ がある sparse relation $R$ の Relational Hash で入力の確率分布が $\mathcal{X}, \mathcal{Y}$ となる方式であり，$H_{R_{lin}}, H'_{R_{lin}}$ がそれぞれ分布 $\mathcal{X}, \mathcal{Y}$ と $\mathsf{RH}_{lin}.\mathsf{KG}$ に関して 2-POW を満たすならば，その Relational Hash 方式は分布 $\mathcal{X}, \mathcal{Y}$ に関して定義 3.6 の偽造不可能性を満たす・

ただし，sparse relation の定義は以下の通りである：

**定義 7.1.** ある関係 $R \subseteq X \times Y \times Z$ が sparse relation であるとは，次の二つの式を満たすことである：

- $X$ 上の分布 $\mathcal{X}$ に関して，どんな PPTA $A_1$ に対しても次の式が成立する：

$$\Pr[x \leftarrow \mathcal{X}; (y,z) \leftarrow A_1(\lambda) : (x,y,z) \in R] < negl(\lambda)$$

- $Y$ 上の分布 $\mathcal{Y}$ に関して，どんな PPTA $A_2$ に対しても次の式が成立する：

$$\Pr[y \leftarrow \mathcal{Y}; (x,z) \leftarrow A_2(\lambda) : (x,y,z) \in R] < negl(\lambda)$$

以下，パート 1 から順に示す.

**補題 7.1.1.** 関係 $R_{lin} = (x,y,z) \mid x+y=z \wedge x,y,z \in \mathbb{F}_2^k$ は $\lambda$-source である分布 $\mathcal{X},\mathcal{Y}$ に関して sparse relation である.

**証明.** 関係 $R_{lin}$ の $x$ と $y$ に関する対称性より分布 $\mathcal{X}$ に関してのみ示せばよい．分布 $\mathcal{X}$ に従いサンプルされた $x$ に対して，ある PPTA $A_1$ が $\lambda$ のみを入力に受け取り $R(x,y,z)=1$ すなわち $y+z=x$ となる $(y,z)$ する確率を考える．このとき，$A_1$ はまさしく $\mathcal{X}$ からサンプルされた $x$ を推測するアルゴリズムである．$\mathcal{X}$ は $\lambda$-source であるから，全ての $x \in X$ について $\Pr[x \mid x \leftarrow \mathcal{X}] \leq 2^{-\lambda}$ となる．以上より，全ての PPTA $A_1$ に対して

$$\Pr[x \leftarrow \mathcal{X}; (y,z) \leftarrow A_1(\lambda) : (x,y,z) \in R] = \max_{x \in X} \Pr[x \mid x \leftarrow \mathcal{X}] < negl(\lambda)$$

□

次に，パート 2 を示す．$H_{R_{lin}}$ と $H'_{R_{lin}}$ は同型であるため，$H_{R_{lin}}$ に関して示せば十分である．まず必要な仮定である $\lambda$-source DDH 仮定と $\lambda$-source Decisional Binary Mix 仮定を導入する.

**仮定 7.2.** $\mathbb{G}$ を位数 $q$ の巡回群とする．$g$ を $\mathbb{G}$ の生成元，$x,y$ を $\mathbb{Z}_q$ 上の $\lambda$-source となる分布からサンプルした値，$z$ を $\mathbb{Z}_q$ 上のランダムな値とすると，次の二つの分布を多項式時間で識別することが困難である：

$$(g, g^x, g^y, g^{xy}) \text{ and } (g, g^x, g^y, g^z)$$

**仮定 7.3.** あるアルゴリズム $\mathcal{G}$ により $(n,q,\mathbb{G})$ が出力されたとする．ただし，$k$ は自然数，$q$ は素数であり，$\mathbb{G}$ は位数 $q$ の群である．$\lambda$-source である $\mathbb{F}_2^n$ 上の分布 $\mathcal{X},\mathcal{Y}$ に関して，$x \leftarrow \mathcal{X}, y \leftarrow \mathcal{Y}, \langle \mathbf{g}_i \rangle_{i=1}^n \leftarrow (\mathbb{G})^n, \langle \mathbf{f}_i \rangle_{i=1}^n \leftarrow (\mathbb{G})^n$ としたとき，次の二つの分布を多項式時間で識別することが困難である：

$$\left( \prod_{i=1}^n \mathbf{g}_i^{(-1)^{x_i}}, \prod_{i=1}^n \mathbf{f}_i^{(-1)^{x_i}} \right) \text{ and } \left( \prod_{i=1}^n \mathbf{g}_i^{(-1)^{x_i}}, \prod_{i=1}^n \mathbf{f}_i^{(-1)^{y_i}} \right)$$

仮定 7.3 は一般的ではない．そこで，この仮定がジェネリックグループモデルで証明可能であることを次の補題で示す.

**補題 7.1.2.** $\lambda$-source Decisional Binary Mix 仮定はジェネリックグループモデルでその困難性が示される．

**証明.** アルゴリズム $A$ とともに次に示すゲームを行うアルゴリズム $B$ を考える．$B$ は $\{0,1\}^m$ から $2n+1$ ビットの文字列を $2n+3$ 個選び，それぞれ $\langle\sigma_g^i\rangle_{i=1}^n, \langle\sigma_f^i\rangle_{i=1}^n, \sigma_g, \sigma_f^0, \sigma_f^1$ として，それらを $A$ に渡す．$B$ の内部では，環 $\mathbb{F}_q[R_1, \cdots, R_n, S_1, \cdots, S_n, T_g, T_{f,0}, T_{f,1}]$ 上の多項式を用いて符号化した要素を保持しておくものとする．

$A$ に与えられた文字列の一貫性を保つために，$B$ は $(F, \sigma)$ の組 $L$ を作成しておく．ただし，$F$ は上で示した環上の多項式であり，$\sigma$ は群の要素である．多項式 $F$ は符号化された要素で示される値を表す．はじめ $L$ は次の値に設定される：

$$L_0 = \left\{ \left\langle \left(R_i, \sigma_g^i\right) \right\rangle_{i=1}^n, \left\langle \left(S_i, \sigma_f^i\right) \right\rangle_{i=1}^n, \left(T_g, \sigma_g\right), \left(T_{f,0}, \sigma_f^0\right), \left(T_{f,1}, \sigma_f^1\right) \right\}$$

アルゴリズム $B$ は群のオラクルを次のようにシミュレートする：

- **群の演算** 二つの文字列 $\sigma_i, \sigma_j$ を与えられたとき，$B$ は対応する二つの多項式 $F_i, F_j$ を復元し $F_i + F_j$ を計算する．もし $F_i + F_j$ が既に $L$ に含まれていた場合には対応する文字列を返す．そうでないならば，新たに（重複がないように）文字列 $\sigma \in \{0,1\}^m$ を選び $(F_i + F_j, \sigma)$ を $L$ に保存する．

- **群の逆元の計算** 文字列 $\sigma$ を与えられたとき，$B$ は対応する多項式 $F$ を復元し $-F$ を計算する．もし $F$ が既に $L$ に含まれていた場合には対応する文字列を返す．そうでないならば，新たに（重複がないように）文字列 $\sigma \in \{0,1\}^m$ を選び $(-F, \sigma)$ を $L$ に保存する．

$A$ はオラクルにクエリした後，ビット $b'$ を出力する．このとき，$B$ はビット $b$，$\mathbb{Z}_q$ から $\langle r_i\rangle_{i=1}^n, \langle s_i\rangle_{i=1}^n$ をランダムに選ぶ．また，$B$ は $\lambda$-source の分布 $\mathcal{X}, \mathcal{Y}$ からそれぞれランダムに $x, y$ を選び，次のように値をセットする：

$$\langle R_i\rangle_{i=1}^n = \langle r_i\rangle_{i=1}^n, \langle S_i\rangle_{i=1}^n = \langle s_i\rangle_{i=1}^n,$$
$$T_g = \sum_{i=1}^n (-1)^{x_i} r_i, T_{f,b} = \sum_{i=1}^n (-1)^{x_i} s_i, T_{f,1-b} = \sum_{i=1}^n (-1)^{y_i} s_i$$

もし $B$ によるシミュレーションが正しいならば $b$ から一切の情報は洩れない．このとき，$A$ が正しく $b$ の値を推測できる確率はちょうど $1/2$ である．一方，$B$ によるシミュレーションが正しくない場合も存在する．これはリスト $L$ の中で異なる多項式が同一の値を取るような衝突が生じるときである．この場合について考える．

$L$ は初め $L_0$ にセットされており，$A$ により群の演算がクエリされるたびにリストに新たな多項式が追加される．しかし，このオラクルの操作によって $L$ に存在する多項式の次数が増えることはない．つまり，どの多項式 $F_i \in L$ も次の形をとる：

$$F_i = \sum_{k=1}^n a_k^i R_k + \sum_{k=1}^n b_k^i S_k + c^i T_g + d^i T_{f,0} + e^i T_{f,1}$$

ただし，$\langle a_k^i \rangle_{k=1}^n, \langle b_k^i \rangle_{k=1}^n, c^i, d^i, e^i$ は $\mathbb{Z}_q$ 上の定数である．ゆえに，二つの異なる多項式 $F_i, F_j$ の値が衝突するのは

$$F_i - F_j = \sum_{k=1}^{n} \left(a_k^i - a_k^j\right) R_k + \sum_{k=1}^{n} \left(b_k^i - b_k^j\right) S_k + \left(c^i - c^j\right) T_g + \left(d^i - d^j\right) T_{f,0} + \left(e^i - e^j\right) T_{f,1}$$

が 0 になるときである．この確率は環 $\mathbb{F}_q\left[R_1, \cdots, R_n, S_1, \cdots, S_n, T_g, T_{f,0}, T_{f,1}\right]$ 上の少なくとも一つの係数が 0 でない多項式

$$F = \sum_{i=1}^{n} a_i R_i + \sum_{i=1}^{n} b_i S_i + cT_g + dT_{f,0} + eT_{f,1}$$

が 0 をとる確率（すなわち $\Pr[F = 0]$）と等しい．ビット $b$ はランダムに選ばれるので $\Pr[F = 0] = 1/2 \Pr[F = 0 \mid b = 0] + 1/2 \Pr[F = 0 \mid b = 1]$ となる．

まずはじめに $\Pr[F = 0 \mid b = 0]$ となる確率について考える．$\lambda$-source である分布 $\mathcal{X}, \mathcal{Y}$ からランダムにサンプルされた $x, y$ に対して，$i$ 番目の要素がそれぞれ $x_i, y_i$ となるベクトルをそれぞれ $\boldsymbol{x}, \boldsymbol{y}$ とすると，

$$\Pr[F = 0 \mid b = 0] = \Pr\left[\sum_{i=1}^{n} \left(a_i + (-1)^{\boldsymbol{x}_i} c\right) R_i + \sum_{i=1}^{n} \left(b_i + (-1)^{\boldsymbol{x}_i} d + (-1)^{\boldsymbol{y}_i} e\right) S_i = 0\right]$$

$\langle a_i \rangle_{i=1}^n, \langle b_i \rangle_{i=1}^n, c, d, e$ の値に応じて上の確率の上限を考える．

**$c \neq 0$ のとき**　ある $u \in \mathbb{F}_2^n$ について $\sum_{i=1}^n \left(a_i + (-1)^{\boldsymbol{x}_i} c\right) R_i = u$ となる確率を考える．$u \neq 0$ とすると少なくとも一つの $i$ について $a_i + (-1)^{x_i} c \neq 0$ である．この確率を $p(\leq 1)$ とすると，$\sum_{i=1}^n \left(a_i + (-1)^{\boldsymbol{x}_i} c\right) R_i = u$ が成立するのは環 $\mathbb{F}_q$ 上からランダムに取得した値が $u$ と一致するときであるので

$$\Pr\left[\sum_{i=1}^{n} \left(a_i + (-1)^{\boldsymbol{x}_i} c\right) R_i = u\right] = p \cdot \frac{1}{q} \leq \frac{1}{q}$$

となる．また $u = 0$ のときは前の確立に加え，全ての $i$ に対して $a_i + (-1)^{x_i} c = 0$ となる場合も成立するため，

$$\Pr\left[\sum_{i=1}^{n} \left(a_i + (-1)^{\boldsymbol{x}_i} c\right) R_i = u\right] \leq \frac{1}{q} + (1 - p) \leq \frac{1}{q} + \frac{1}{2^\lambda}$$

となる．なぜなら $x$ は $\lambda$-source である分布からサンプルされた値である．

**$c = 0$ かつ $a_{i^*} \neq 0$ となる $i^*$ が存在するとき**　どのような $u \in \mathbb{F}_2^n$ に対しても

$$\Pr\left[\sum_{i=1}^{n} \left(a_i + (-1)^{\boldsymbol{x}_i} c\right) R_i = u\right] = \frac{1}{q}$$

が成立する．

$c = 0$ **かつ** $\forall i; a_i = 0$ **で** $d \neq 0, e \neq 0$ **のとき** ある $u \in \mathbb{F}_2^n$ について次の式が成立する確率を考える：$\sum_{i=1}^{n} (b_i + (-1)^{\boldsymbol{x}_i} d + (-1)^{\boldsymbol{y}_i} e) S_i = u$．$c = 0$ のときと同様の議論で $u \neq 0$ のときはこの確率は高々 $\frac{1}{q}$ である．$u = 0$ の場合も考慮すると，$S_i$ の係数が全て 0 である場合も含められる．$x, y$ は両者とも $\lambda$-source である分布からサンプルされた値であるため，この確率は高々 $\frac{1}{2^\lambda} \cdot \frac{1}{2^\lambda} = \frac{1}{4^\lambda}$ となる．まとめると，どんな $u \in \mathbb{F}_2^n$ についても

$$\Pr\left[\sum_{i=1}^{n} (b_i + (-1)^{\boldsymbol{x}_i} d + (-1)^{\boldsymbol{y}_i} e) S_i = u\right] \leq \frac{1}{q} + \frac{1}{4^\lambda}$$

が成立する．

$c = 0$ **かつ** $\forall i; a_i = 0$ **で** $d = 0, e \neq 0$ **のとき** $c = 0$ の場合と全く同様の議論から，どのような $u \in \mathbb{F}_2^n$ に対しても

$$\Pr\left[\sum_{i=1}^{n} (b_i + (-1)^{\boldsymbol{x}_i} d + (-1)^{\boldsymbol{y}_i} e) S_i = u\right] \leq \frac{1}{q} + \frac{1}{2^\lambda}$$

が成立する．

$c = 0$ **かつ** $\forall i; a_i = 0$ **で** $d \neq 0, e = 0$ **のとき** $c = 0$ の場合と全く同様の議論から，どのような $u \in \mathbb{F}_2^n$ に対しても

$$\Pr\left[\sum_{i=1}^{n} (b_i + (-1)^{\boldsymbol{x}_i} d + (-1)^{\boldsymbol{y}_i} e) S_i = u\right] \leq \frac{1}{q} + \frac{1}{2^\lambda}$$

が成立する．

$c = 0$ **かつ** $\forall i; a_i = 0, d = 0, e = 0$ **のとき** 少なくとも $b_{j^*} \neq 0$ となるような $i^*$ が存在する．（そうでない場合，多項式 $F$ の係数が全て 0 になってしまう．）ゆえに，どのような $u \in \mathbb{F}_2^n$ に対しても

$$\Pr\left[\sum_{i=1}^{n} (b_i + (-1)^{\boldsymbol{x}_i} d + (-1)^{\boldsymbol{y}_i} e) S_i = u\right] = \frac{1}{q}$$

が成立する．

以上すべての場合に関して

$$\begin{aligned}\Pr[F = 0 \mid b = 0] &= \Pr\left[\sum_{i=1}^{n} (a_i + (-1)^{\boldsymbol{x}_i} c) R_i + \sum_{i=1}^{n} (b_i + (-1)^{\boldsymbol{x}_i} d + (-1)^{\boldsymbol{y}_i} e) S_i = 0\right] \\ &\leq \frac{1}{q} + \frac{1}{2^\lambda}\end{aligned}$$

が成立する．この議論は $b=1$ のときも成立するため

$$\Pr[F=0 \mid b=1] \leq \frac{1}{q}+\frac{1}{2^{\lambda}}$$

ゆえに

$$\Pr[F=0] \leq \frac{1}{q}+\frac{1}{2^{\lambda}}$$

□

**補題 7.1.3.** 構成 Π の $H_{R_{lin}}$ は，$\lambda$-source Decisional Binary Mix 仮定と DDH 仮定のもとで，$\lambda$-source である分布 $\mathcal{X}$ と鍵生成アルゴリズム $\mathsf{RH}_{lin}.\mathsf{KG}$ の出力分布 $\mathcal{K}$ に関して定義 3.4 の 2-POW を満たす．

**証明.** $\boldsymbol{g}_0 \leftarrow \mathbb{G}_1, \boldsymbol{h}_0 \leftarrow \mathbb{G}_2, \langle a_i\rangle_{i=1}^{k+1}, \langle b_i\rangle_{i=1}^{k+1} \leftarrow \mathbb{Z}_q^*$ をそれぞれランダムに選び，$\boldsymbol{g}_i := \boldsymbol{g}_0^{a_i}, \boldsymbol{h}_i := \boldsymbol{h}_0^{b_i}, pk_R := \sum_{i=1}^{k+1} a_i b_i, pk := (\langle \boldsymbol{g}_i\rangle_{i=0}^{k+1}, \langle \boldsymbol{h}_i\rangle_{i=0}^{k+1}, pk_R), pk_R := \sum_{i=1}^{k+1} a_i b_i$ としたとき，$\lambda$-source Decisional Binary Mix 仮定と DDH 仮定のもとで，次に示す二つの分布 $\Delta_0, \Delta_1$ が計算量的に識別不可能であればよい．ただし，$r, s \leftarrow \mathbb{Z}_q^*$ はランダムに選ばれ $x, y$ はそれぞれ $\lambda$-source である分布 $\mathcal{X}, \mathcal{Y}$ に従ってサンプルされるものとする：

$$\Delta_0 = \left(pk,\quad \boldsymbol{g}_0^r, \left\langle \boldsymbol{g}_i^{(-1)^{x_i} r}\right\rangle_{i=1}^{k}, \boldsymbol{g}_{k+1}^r,\quad \boldsymbol{g}_0^s, \left\langle \boldsymbol{g}_i^{(-1)^{x_i} s}\right\rangle_{i=1}^{k}, \boldsymbol{g}_{k+1}^s\right),$$
$$\Delta_1 = \left(pk,\quad \boldsymbol{g}_0^r, \left\langle \boldsymbol{g}_i^{(-1)^{x_i} r}\right\rangle_{i=1}^{k}, \boldsymbol{g}_{k+1}^r,\quad \boldsymbol{g}_0^s, \left\langle \boldsymbol{g}_i^{(-1)^{y_i} s}\right\rangle_{i=1}^{k}, \boldsymbol{g}_{k+1}^s\right)$$

まず初めに，次の二つの分布が計算量的に識別不可能であることを示す：

$$Dist_0 := \left(\boldsymbol{g}_0, \langle \boldsymbol{g}_i\rangle_{i=1}^{k},\quad \boldsymbol{g}_0^r, \left\langle \boldsymbol{g}_i^{(-1)^{x_i}}\right\rangle_{i=1}^{k}, \prod_{i=1}^{k} \boldsymbol{g}_i^r,\quad \boldsymbol{g}_0^s, \left\langle \boldsymbol{g}_i^{(-1)^{x_i} s}\right\rangle_{i=1}^{k}, \prod_{i=1}^{k} \boldsymbol{g}_i^s\right),$$
$$Dist_0' := \left(\boldsymbol{g}_0, \langle \boldsymbol{g}_i\rangle_{i=1}^{k},\quad \boldsymbol{f}_0, \langle \boldsymbol{f}_i\rangle_{i=1}^{k}, \prod_{i=1}^{k} \boldsymbol{f}_i^{(-1)^{x_i}},\quad \boldsymbol{h}_0, \langle \boldsymbol{h}_i\rangle_{i=1}^{k}, \prod_{i=1}^{k} \boldsymbol{h}_i^{(-1)^{x_i}}\right)$$

ただし，$\boldsymbol{g}_i, \boldsymbol{f}_i, \boldsymbol{h}_i$ はそれぞれ独立に選ばれるものとする．ここで

$$Dist_{0,l} := \left(\begin{array}{c} \boldsymbol{g}_0, \langle \boldsymbol{g}_i\rangle_{i=1}^{k} \\ \boldsymbol{g}_0^r, \left\langle \boldsymbol{g}_i^{(-1)^{x_i} r}\right\rangle_{i=1}^{l-1}, \langle \boldsymbol{f}_i\rangle_{i=l}^{k}, \prod_{i=1}^{l-1} \boldsymbol{g}_i^r \cdot \prod_{i=l}^{k} \boldsymbol{f}_i^{(-1)^{x_i}} \\ \boldsymbol{g}_0^s, \left\langle \boldsymbol{g}_i^{(-1)^{x_i} s}\right\rangle_{i=1}^{l-1}, \langle \boldsymbol{h}_i\rangle_{i=l}^{k}, \prod_{i=1}^{l-1} \boldsymbol{g}_i^s \cdot \prod_{i=l}^{k} \boldsymbol{h}_i^{(-1)^{x_i}} \end{array}\right)$$

とおくと，$Dist_{0,k+1} = Dist_0, Dist_{0,1} = Dist_0'$ となる．

$(\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{u}^r, \boldsymbol{w})$ を $\lambda$-source DDH インスタンスとすると，$\boldsymbol{w}$ が $\boldsymbol{v}^r$ と等しいか識別することが困難である．ここで，次の分布を考える．ただし，$s, u_i$ は全て $\mathbb{Z}_q^*$ から，

$\boldsymbol{f}_i, \boldsymbol{h}_i$ は全て $\mathbb{G}_1$ からランダムに選ばれるものとし，$x$ は $\mathbb{F}_2^k$ 上の $\lambda$-source となる分布からサンプルされるものとする：

$$Dist_{0,l,DDH} := \left( \begin{array}{c} \boldsymbol{u}, \langle \boldsymbol{u}^{u_i} \rangle_{i=1}^{l-1}, \boldsymbol{v}, \langle \boldsymbol{u}^{u_i} \rangle_{i=l+1}^{k}, \\ \boldsymbol{u}^r, \left\langle \boldsymbol{u}^{r(-1)^{x_i} u_i} \right\rangle_{i=1}^{l-1}, \boldsymbol{w}^{(-1)^{x_l}}, \langle \boldsymbol{f}_i \rangle_{i=l+1}^{k}, \prod_{i=1}^{l-1} \boldsymbol{u}^{r u_i} \cdot \boldsymbol{w} \cdot \prod_{i=l+1}^{k} \boldsymbol{f}_i^{(-1)^{x_i}}, \\ \boldsymbol{u}^s, \left\langle \boldsymbol{u}^{s(-1)^{x_i} u_i} \right\rangle_{i=1}^{l-1}, \langle \boldsymbol{h}_i \rangle_{i=l}^{k}, \prod_{i=1}^{l-1} \boldsymbol{u}^{s u_i} \cdot \prod_{i=l}^{k} \boldsymbol{h}_i^{(-1)^{x_i}} \end{array} \right)$$

今，$\boldsymbol{w}$ がランダムな値であったならば $\boldsymbol{f_l} = \boldsymbol{w}^{(-1)^{x_l}}$ とみなすことができるので $Dist_{0,l,DDH}$ の分布は $Disk_{0,l}$ の分布と等しくなる．また，$\boldsymbol{w} = \boldsymbol{v}^r$ となる場合には，$\boldsymbol{w}^{(-1)^{x_l}} = \boldsymbol{v}^{r(-1)^{x_l}} = \boldsymbol{u}^{r(-1)^{x_l} u_l}$ とみなすことができるので $Dist_{0,l,DDH}$ の分布は次の分布と等しくなる：

$$Dist_{0,l+1/2} := \left( \begin{array}{c} \boldsymbol{g}_0, \langle \boldsymbol{g}_i \rangle_{i=1}^{k}, \\ \boldsymbol{g}_0^r, \left\langle \boldsymbol{g}_i^{(-1)^{x_i} r} \right\rangle_{i=1}^{l}, \langle \boldsymbol{f}_i \rangle_{i=l+1}^{k}, \prod_{i=1}^{l} \boldsymbol{g}_i^r \cdot \prod_{i=l+1}^{k} \boldsymbol{f}_i^{(-1)^{x_i}} \\ \boldsymbol{g}_0^s, \left\langle \boldsymbol{g}_i^{(-1)^{x_i}} \right\rangle_{i=1}^{l-1}, \langle \boldsymbol{h}_i \rangle_{i=l}^{k}, \prod_{i=1}^{l-1} \boldsymbol{g}_i^s \cdot \prod_{i=l}^{k} \boldsymbol{h}_i^{(-1)^{x_i}} \end{array} \right)$$

$\lambda$-source DDH の難しさより $Dist_{0,l+1/2} \approx_{DDH} Dist_{0,l}$ となるため，$Dist_{0,l-1} \approx_{DDH} Dist_{0,l}$ となる．これを繰り返し用いることで $Dist_0 = Dist_{0,k+1} \approx_{DDH} \cdots \approx_{DDH} Dist_{0,1} = Dist'_0$ を得る．

次に，以下の二つの分布も計算量的に識別不可能であることを示す：

$$Dist_1 := \left( \boldsymbol{g}_0, \langle \boldsymbol{g}_i \rangle_{i=1}^{k}, \quad \boldsymbol{g}_0^r, \left\langle \boldsymbol{g}_i^{(-1)^{x_i}} \right\rangle_{i=1}^{k}, \prod_{i=1}^{k} \boldsymbol{g}_i^r, \quad \boldsymbol{g}_0^s, \left\langle \boldsymbol{g}_i^{(-1)^{y_i} s} \right\rangle_{i=1}^{k}, \prod_{i=1}^{k} \boldsymbol{g}_i^s \right),$$

$$Dist'_1 := \left( \boldsymbol{g}_0, \langle \boldsymbol{g}_i \rangle_{i=1}^{k}, \quad \boldsymbol{f}_0, \langle \boldsymbol{f}_i \rangle_{i=1}^{k}, \prod_{i=1}^{k} \boldsymbol{f}_i^{(-1)^{x_i}}, \quad \boldsymbol{h}_0, \langle \boldsymbol{h}_i \rangle_{i=1}^{k}, \prod_{i=1}^{k} \boldsymbol{h}_i^{(-1)^{y_i}} \right)$$

ただし，$\boldsymbol{g}_i, \boldsymbol{f}_i, \boldsymbol{h}_i$ はそれぞれ独立に選ばれるものとする．これは先ほどと同様の手法を用いることで $Dist_1 \approx_{DDH} Dist'_1$ を証明できる．

今，$\lambda$-source Decisional Binary Mix 仮定より，$Dist'_0 \approx_{DecisionalBinaryMix} Dist'_1$ となるので，$Dist_0 \approx_{DDH, DecisionalBinaryMix} Dist_1$ が得られる．

最後に，二つの分布 $\Delta_0, \Delta_1$ を識別可能な攻撃者 $A$ は $Dist_0$ と $Dist_1$ を識別可能であることを示すことで，矛盾により $\Delta_0, \Delta_1$ が識別不可能であることを示す．$A$ を用いて $Dist_0$ と $Dist_1$ を識別するアルゴリズム $B$ を作成する．$Dist_0$ と $Dist_1$ を識別することは

$$\left( \boldsymbol{g}_0, \langle \boldsymbol{g}_i \rangle_{i=1}^{k}, \quad \boldsymbol{g}_0^r, \left\langle \boldsymbol{g}_i^{(-1)^{x_i} r} \right\rangle_{i=1}^{k}, \prod_{i=1}^{k} \boldsymbol{g}_i^r, \quad \boldsymbol{g}_0^s, \left\langle \boldsymbol{g}_i^{(-1)^{z_i}} \right\rangle_{i=1}^{k}, \prod_{i=1}^{k} \boldsymbol{g}_i^s \right)$$

を与えられて，$z = x$ かどうかを識別する問題にほかならない．上の値を与えられた $B$ はまず $u, s, \langle u_i \rangle_{i=1}^{k}$ をそれぞれ $\mathbb{Z}_q^*$ からランダムに選ぶ．また $\boldsymbol{h}_0$ を $\mathbb{G}_2$ からランダムに選び，$pk := (pk_1, pk_2, pk_R)$ を次のように定義する：

$$pk_1 := \boldsymbol{g}_0, \left\langle \boldsymbol{g}_i^{u_i^{-1}} \right\rangle_{i=1}^{k}, \boldsymbol{g}_0^u \prod_{i=1}^{k} \boldsymbol{g}_i^{-1}, \quad pk_2 := \boldsymbol{h}_0, \langle \boldsymbol{h}_0^{u_i s} \rangle_{i=1}^{k}, \boldsymbol{h}_0^s, \quad pk_R := us$$

このとき，$\boldsymbol{g}_0, \left\langle \boldsymbol{g}_i^{u_i^{-1}} \right\rangle_{i=1}^{k}, \boldsymbol{h}_0, \langle \boldsymbol{h}_0^{u_i s} \rangle_{i=1}^{k}, \boldsymbol{h}_0^s, us$ はそれぞれ独立の集合からランダムに選ばれた値であり，$\boldsymbol{g}_0^u \prod_{i=1}^{k} \boldsymbol{g}_i^{-1}$ はこれらの値により決定的に決まる．ゆえに，この $pk$ の分布は 関係 $R_{lin}$ の Relational Hash 方式の $pk$ の分布と等しくなる．$B$ は次の値を $A$ にクエリする：

$$Tuple := \left( \begin{array}{c} pk, \\ \boldsymbol{g}_0^r, \left\langle \boldsymbol{g}_i^{(-1)^{x_i} r \cdot u_i^{-1}} \right\rangle_{i=1}^{k}, \boldsymbol{g}_0^{r \cdot u} \left( \prod_{i=1}^{k} \boldsymbol{g}_i^r \right)^{-1} \\ \boldsymbol{g}_0^s, \left\langle \boldsymbol{g}_i^{(-1)^{z_i} s \cdot u_i^{-1}} \right\rangle_{i=1}^{k}, \boldsymbol{g}_0^{s \cdot u} \left( \prod_{i=1}^{k} \boldsymbol{g}_i^s \right)^{-1} \end{array} \right)$$

これは $z = x$ のとき $\Delta_0$ であり，そうでないならば $\Delta_1$ に一致する．すなわち，$A$ は $z = x$ かどうかを判定できるので，$B$ も $z = x$ かどうかを判定できることになる．これは $Dist_0$ と $Dist_1$ が識別不可能であることに矛盾する．以上より，$\Delta_0$ と $\Delta_1$ は計算量的に識別不可能であり，構成 $\Pi$ の $H_{R_{lin}}$ は 2-POW を満たす．　□

最後に，パート 3 を示す．

**補題 7.1.4.** $(\mathsf{RH}_{lin}.\mathsf{KG}, H_{R_{lin}}, H'_{R_{lin}}, \mathsf{RH}_{lin}.\mathsf{Ver})$ がある sparse relation $R$ の Relational Hash で入力の確率分布が $\mathcal{X}, \mathcal{Y}$ となる方式であり，$H_{R_{lin}}, H'_{R_{lin}}$ がそれぞれ分布 $\mathcal{X}, \mathcal{Y}$ と $\mathsf{RH}_{lin}.\mathsf{KG}$ に関して 2-POW を満たすならば，その Relational Hash 方式は分布 $\mathcal{X}, \mathcal{Y}$ に関して定義 3.6 の偽造不可能性を満たす．

**証明.** この方式が偽造不可能性を満たさないとする．すなわち，$x \leftarrow \mathcal{X}$ について $(pk, H_{R_{lin}}(pk, x, r))$ が与えられたとき，無視可能でない確率で $R(x, y, z) = 1$ となる $H'_{R_{lin}}(pk, y, s)$ と $z$ を出力する攻撃者 $A$ が存在するとする．この $A$ を用いると $(pk, H_{R_{lin}}(pk, x, r_1), H_{R_{lin}}(pk, x, r_2))$ と $(pk, H_{R_{lin}}(pk, x, r_1), H_{R_{lin}}(pk, x', r_2))$ が無視可能でない確率で識別可能な攻撃者 $B$ を構成可能である．$B$ は $(pk, H_{R_{lin}}(pk, x, r_1), H_{R_{lin}}(pk, w, r_2))$ を受け取ると $(pk, x, r_1)$ を $A$ にクエリする．$A$ は無視可能でない確率で $R(x, y, z) = 1$ となる $H'_{R_{lin}}(pk, y, s)$ と $z$ を出力する．それらを受け取った $B$ は $\mathsf{RH}_{lin}.\mathsf{Ver}(pk, H_{R_{lin}}(pk, w, r_2), H'_{R_{lin}}(pk, y, s), z)$ を計算することにより $R(w, y, z)$ の値を調べる．$w = x$ ならば常に $R(w, y, z) = 1$ となり，$w \neq x$ ならば $R(w, y, z) = 0$ となる確率が高い（なぜならば $R$ は sparse relation であるため $w \neq x$ となる $w$ と $R(w, y, z) = 1$ となる $(y, z)$ を求められる確率が無視可能）．ゆえに $B$ は $w$ の値が $x$ と等しいかそうでないか識別することができ，これはまさしく $H_{R_{lin}}$ の 2-POW を破る攻撃である．対偶より題意は示された．　□

以上より，構成 $\Pi_{lin} = (\mathsf{RH}_{lin}.\mathsf{KG}, H_{R_{lin}}, H'_{R_{lin}}, \mathsf{RH}_{lin}.\mathsf{Ver})$ は $\lambda$-source に関する偽造不可能性を満たす．　□

### (ii) $\lambda$-source に関する偽造不可能性を満たす関係 $R_\delta$ の Relational hash

(i) で示した linear Relational Hash の構成 $\Pi_{lin}$ と定義 3.1 の $(n, k, 2\delta+1)$ linear ECC を組み合わせることで，関係 $R_\delta = \{dist(x, y) \leq \delta \wedge x, y \in \mathbb{F}_2^n\}$ の Relational Hash 方式 $\Pi_{dist} = (\mathsf{RH}.\mathsf{KG}, H_R, H'_R, \mathsf{RH}.\mathsf{Ver})$ を構成する．構成は以下のようになる：

$\mathsf{RH.KG}(1^\lambda)$：$(n, k, 2\delta+1)$ linear ECC $\mathcal{C}$ = (ENCODE,DECODE) を選ぶ．ただし，$k = O(\lambda)$ とする．$\mathsf{RH}_{lin}.\mathsf{KG}(1^\lambda)$ を実行し $pk_{lin}$ を計算し，次の $pk$ を出力する：

$$pk := (\text{ENCODE, DECODE, } pk_{lin})$$

$H_R(pk, x)$：$x \in \mathbb{F}_2^n$ と $pk = (\text{ENCODE, DECODE, } pk_{lin})$ を入力として受け取り，次の $hx := (hx_1, hx_2)$ を出力する：

$$hx_1 := x + \text{ENCODE}(r), hx_2 := H_{R_{lin}}(pk_{lin}, r)$$

ただし，$r \leftarrow \mathbb{F}_2^k$ とする．

$H'_R(pk, y)$：$y \in \mathbb{F}_2^n$ と $pk = (\text{ENCODE, DECODE, } pk_{lin})$ を入力として受け取り，次の $hy := (hy_1, hy_2)$ を出力する：

$$hy_1 := y + \text{ENCODE}(s), hy_2 := H_{R_{lin}}(pk_{lin}, s)$$

ただし，$s \leftarrow \mathbb{F}_2^k$ とする．

$\mathsf{RH.Ver}(pk, hx, hy, \delta)$:$pk = (\text{ENCODE, DECODE, } pk_{lin})$ および $hx = (hx_1, hx_2), hy = (hy_1, hy_2)$ を入力として受け取り，$z = \text{DECODE}(hx_1 + hy_1)$ を計算する．DECODE に失敗したとき，もしくは $dist(\text{ENCODE}(z), hx_1 + hy_1) > \delta$ のとき 0 を出力する．それ以外の場合は $\mathsf{RH}_{lin}.\mathsf{Ver}(pk_{lin}, hx_2, hy_2, z)$ を出力する．

$dist(x, y) \leq \delta$ のとき，$z = r + s$ となる．$\mathcal{C}$ は linear ECC であるから，$\text{ENCODE}(z) = \text{ENCODE}(r) + \text{ENCODE}(s)$ より $dist(\text{ENCODE}(z), hx_1 + hy_1) \leq \delta$ となる．また $\Pi_{lin}$ の正当性より $\mathsf{RH}_{lin}.\mathsf{Ver}(pk_{lin}, hx_2, hy_2, z) = 1$ となるため，この方式も正当性を満たす．

**定理 7.2.** linear Relational Hash 方式 $\Pi_{lin}$ が $\lambda$-source となる $\mathbb{F}_2^k$ 上の分布 に関する偽造不可能性を満たすならば，方式 $\Pi_{dist}$ も $\lambda$-source となる $\mathbb{F}_2^n$ 上の分布 に関する偽造不可能性を満たす．

**証明.** 方式 $\Pi_{dist}$ の $\lambda$-source となる $\mathbb{F}_2^n$ 上の分布に関する偽造不可能性を無視可能でない確率で破る攻撃者 $A$ が存在すると仮定する．このとき，$A$ を用いて方式 $\Pi_{lin}$ の $\lambda$-source となる $\mathbb{F}_2^k$ 上の分布に関する偽造不可能性を無視可能でない確率で破る攻撃者 $B$ を作ることができることを示す．

$B$ はある乱数 $r \leftarrow \mathbb{F}_2^k$ について $(pk_{lin}, hx_{lin} = H_{R_{lin}}(pk_{lin}, r))$ を与えられるものとする．ここで $B$ は $\lambda$-source となる $\mathbb{F}_2^n$ 上の分布から $x'$ をサンプルし，$pk := (\text{ENCODE}, \text{DECODE}, pk_{lin})$ と $hx := (x', hx_{lin})$ を $A$ にクエリする（このとき $hx$ は $m \leftarrow \mathbb{F}_2^n$ について $H_R(pk, m)$ を計算した値と識別不可能である）．$A$ が $hy' := (y', hy_{lin})$ を出力したとすると，正当性より $\mathsf{RH.Ver}(pk, hx, hy', \delta) = 1$ となる．このとき常に $\mathsf{RH}_{lin}.\mathsf{Ver}(pk_{lin}, hx_{lin}, hy_{lin}, \text{DECODE}(x' + y')) = 1$ となるので，$B$ は $(hy_{lin}, \text{DECODE}(x' + y'))$ を出力すれば無視可能でない確率で偽造不可能性を破ることができる．これは仮定に矛盾するため，定理 7.2 は示された．　□

## 7.4　弱衝突困難性を満たす確率的ハッシュ

ここでは，前節で示した構成 $\Pi_{dist}$ に含まれる確率的ハッシュ $H_R$ が定義 6.2 の弱衝突困難性を満たすことを示す．$H_R$ の構成を改めて記す．$K_\lambda$ を鍵空間，$Rand_\lambda$ を乱数空間としたとき， $H_R$ は鍵 $pk = (\mathrm{ENCODE}, \mathrm{DECODE}, pk_{lin}) \in K_\lambda$, 入力 $x \in \mathbb{F}_2^n$ を入力として受け取り，次で計算される $hx := (hx_1, hx_2)$ を出力する．

$$hx_1 := x + \mathrm{ENCODE}(r), hx_2 := H_{R_{lin}}(pk_{lin}, r)$$

ただし，$r \leftarrow Rand_\lambda$ とする．

**定理 7.3.** 上で示した $H_R$ は定義 6.2 の弱衝突困難性を満たす．

**証明.** $H_R$ の弱衝突困難性に対する攻撃者 $A$ が存在すると仮定する．このとき $A$ は $(x + \mathrm{ENCODE}(r), H_{R_{lin}}(r)) = (y + \mathrm{ENCODE}(s), H_{R_{lin}}(s))$ となる $(x, y, r, s)$ を出力する．$H_{R_{lin}}(pk_{lin}, r)$ の構成を改めて記述すると，ランダムに $t \in \mathbb{Z}_q^*$ をサンプルし $\left(\boldsymbol{g}_0^t, \left\langle \boldsymbol{g}_i^{(-1)^{r_i} t} \right\rangle_{i=1}^{k}, \boldsymbol{g}_{k+1}^t\right)$ を出力する．ただし $r_i$ は $r$ の $i$ ビット目の値を表す．今，$A$ は $H_{R_{lin}}(pk_{lin}, r) = H_{R_{lin}}(pk_{lin}, s)$ となる $r, s$ を出力する．すなわち，$t, u \leftarrow \mathbb{Z}_q^*$ に対して，$\left(\boldsymbol{g}_0^t, \left\langle \boldsymbol{g}_i^{(-1)^{r_i} t} \right\rangle_{i=1}^{k}, \boldsymbol{g}_{k+1}^t\right)$ と $\left(\boldsymbol{g}_0^u, \left\langle \boldsymbol{g}_i^{(-1)^{s_i} u} \right\rangle_{i=1}^{k}, \boldsymbol{g}_{k+1}^u\right)$ が等しくなる．これは $r, s$ の値を問わず，少なくともランダムにサンプルされた $t, u \in \mathbb{Z}_q^*$ が等しくなる必要がある．その確率は $1/q$ であり，今 $q$ はセキュリティパラメータの指数サイズであるから，$A$ の攻撃成功確率は無視可能な確率である． □

# Chapter 8　結論

本研究では，サイバーフィジカル系における理論的な安全性解析の基盤として，既存の暗号理論的枠組みを拡張し，それを用いたモノの電子署名方式とその安全性定義を 2 つ提案した．また，それらを満たす構成も示した．

既存の暗号理論的枠組みを損なうことなく物理空間へ拡張する手法として，オラクルチューリングマシンの考えを応用した．すなわち，計算機上で物理空間での操作を記述するのは限界がある [20] ため，そうした操作を表すオラクルを方式に与えることで，その方式内では実行可能な物理空間での操作がアルゴリズム (PEA) として定式化できるようになった．具体的な操作としては，新たな物体を生成するコマンドと対応する電子データを得るセンシングを導入した．PEA に関しては 7.2 節で議論した通り仮定として与える部分が大きく，その仮定の解析は数学的には困難であるためヒューリスティックな議論にならざるを得ない．

また， PEA を用いることでモノの電子署名の定式化を行った．シンタックスは従来の電子署名と同様であるが，攻撃者の攻撃能力として PEA を考えるため，安全性定義で考えるゲーム内での攻撃者の振る舞いに差異が生じた．方式としてはセンシングデータに対して署名を作成するという直感的な構成が偽造不可能性を示す EUF-COA を満たすことを示した．その安全性は基盤とする電子署名方式の EUF-CMA 安全性に帰着される．また，モノの電子署名特有の問題として，サイバー空間にいる攻撃者が手に入れた署名から物体を特定できてしまうとその署名を用いた偽造が行われる可能性があることを指摘した．この攻撃に対する安全性としてモノの秘匿性を定義し，方式としてセンシングデータの確率的ハッシュに対して署名を行うという構成であればモノの秘匿性を満たすことを示した．ただし，署名と検証で用いる確率的ハッシュの組は Relational Hash である必要があり，その EUF-COA 安全性は基盤とする電子署名方式の EUF-CMA 安全性と確率的ハッシュの弱衝突困難性に，モノの秘匿性は Relational Hash の偽造不可能性に帰着できることを示した．最後に，上記の仮定に用いた，弱衝突困難性を満たす確率的ハッシュの組で偽造不可能性を満たす Relational Hash の存在もジェネリックグループモデルで示した．

# 謝辞

本研究にあたり，日ごろから密にご指導いただきました東京大学生産技術研究所の松浦幹太教授に心から感謝申し上げます．松浦先生には，研究に取り組むにあたり必要となるような日ごろから取り組むべき細かな内容から研究の大局を見て進むべき指針の助言までいただき，数え切れないほどの有意義な学びを得ることができました．また，学会参加などの各種活動の機会も与えていただいたこともあり，修士課程 2 年間を非常に有意義に過ごすことができました．改めて深く感謝申し上げます。

また，研究に関して大いに助言をいただきました産業技術総合研究所サイバーフィジカルセキュリティ研究センター高機能暗号研究グループの花岡悟一郎さん，Nuttapong Attrapadung さん，Jacob Schuldt さん，松田隆宏さん，山田翔太さん，勝又秀一さん，坂井祐介さん，照屋唯紀さん，横浜国立大学の松本勉教授には深く感謝いたします．特に花岡さん，山田さん，勝又さん，坂井さんには論文執筆や発表資料の作成など細部までご助言いただきました．

そして，研究室での研究活動を円滑に進める上で常に協力を惜しまず支えて下さった松浦研究室秘書の鶴山陽子さんに心から感謝申し上げます．

さらに，松浦研究室のメンバーである，細井琢朗さん，島田要さん，宮前剛さん，林田淳一郎さん，Kittiphop Phalakarn さん，石井龍さん，浅野泰輝さん，久野朔さん，かつてメンバーであった碓井利宜さん，角田大輔さん，宮里俊太郎さんには，主に研究室打ち合わせにおいて，活発に議論をしたり有意義な助言をいただきました．深く感謝申し上げます．特に林田さんには論文執筆において基本作法のような細かい点までご助言いただきました．

最後になりますが，松浦研究室での研究打ち合わせ，および産業技術総合研究所での勉強会の参加者の皆様，常日頃から支えてくれた家族，修士課程を過ごす中でお世話になりました全ての方々に感謝申し上げます．

# 参考文献


[1] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions. Cryptology ePrint Archive, Report 2005/254, 2005. `https://ia.cr/2005/254`.

[2] Mark Manulis Martijn Stam Alexander W. Dent, Marc Fischlin and Dominique Schroder. Confidential signatures and deterministic signcryption. Cryptology ePrint Archive, Report 2009/588, 2009. `https://ia.cr/2009/588`.

[3] Frederik Armknecht, Roel Maes, Ahmad-Reza Sadeghi, Berk Sunar, and Pim Tuyls. Memory leakage-resilient encryption based on physically unclonable functions. In *Towards Hardware-Intrinsic Security*, pages 135–164. Springer, 2010.

[4] Monika Bansal, Munish Kumar, and Manish Kumar. 2d object recognition techniques: state-of-the-art work. *Archives of Computational Methods in Engineering*, pages 1–15, 2020.

[5] George Baryannis, Samir Dani, and Grigoris Antoniou. Predicting supply chain risks using machine learning: The trade-off between performance and interpretability. *Future Generation Computer Systems*, 101:993–1004, 2019.

[6] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In Christian Cachin and Jan L. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, pages 506–522, Berlin, Heidelberg, 2004. Springer.

[7] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In *International Conference on the Theory and Application of Cryptology and Information security*, pages 514–532. Springer, 2001.

[8] Dan Boneh, Ananth Raghunathan, and Gil Segev. Function-private identity-based encryption: Hiding the function in functional encryption. Cryptology ePrint Archive, Report 2013/283, 2013. `https://ia.cr/2013/283`.

[9] Ran Canetti. Towards realizing random oracles: Hash functions that hide all partial information. Cryptology ePrint Archive, Report 1997/007, 1997. `https://ia.cr/1997/007`.

[10] Ran Canetti, Daniele Micciancio, and Omer Reingold. Perfectly one-way probabilistic hash functions (preliminary version). In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, pages 131–140, New York, NY, USA, 1998. Association for Computing Machinery.

[11] Aldar C-F. Chan and Ian F. Blake. Conditionally verifiable signatures. Cryptology ePrint Archive, Report 2005/149, 2005. `https://ia.cr/2005/149`.

[12] David Chaum and Hans van Antwerpen. Undeniable signatures. In Gilles Brassard, editor, *Advances in Cryptology — CRYPTO' 89 Proceedings*, pages 212–216, New York, NY, 1990. Springer New York.

[13] Ilya Sutskever Joan Bruna Dumitru Erhan Ian Goodfellow Rob Fergus Christian Szegedy, Wojciech Zaremba. Intriguing properties of neural networks. ArXiv prePrint, arXiv:1312.6199, 2014. `https://arxiv.org/abs/1312.6199`.

[14] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644–654, 1976.

[15] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Information Theory*, 31(4):469–472, 1985.

[16] Nils Fleischhacker, Felix Günther, Franziskus Kiefer, Mark Manulis, and Bertram Poettering. Pseudorandom signatures. Cryptology ePrint Archive, Report 2011/673, 2011. `https://ia.cr/2011/673`.

[17] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, 18(1):186–208, 1989.

[18] Shafi Goldwasser, Silvio Micali, and Ronald L Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, 1988.

[19] Yulan Guo, Mohammed Bennamoun, Ferdous Sohel, Min Lu, and Jianwei Wan. 3d object recognition in cluttered scenes with local surface features: A survey. *IEEE TPAMI*, 36(11):2270–2287, 2014.

[20] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptographic sensing. Cryptology ePrint Archive, Report 2019/637, 2019. `https://ia.cr/2019/637`.

[21] Ik Rae Jeong, Jeong Ok Kwon, Dowon Hong, and Dong Hoon Lee. Constructing peks schemes secure against keyword guessing attacks is possible? *Computer Communications*, 32(2):394–396, 2009.

[22] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1(1):36–63, 2001.

[23] Kamil Kluczniak. Domain-specific pseudonymous signatures revisited. Cryptology ePrint Archive, Report 2016/070, 2016. `https://ia.cr/2016/070`.

[24] Hau L Lee and Seungjin Whang. Higher supply chain security with lower cost: Lessons from total quality management. *International Journal of Production Economics*, 96(3):289–300, 2005.

[25] Li Liu, Wanli Ouyang, Xiaogang Wang, Paul Fieguth, Jie Chen, Xinwang Liu, and Matti Pietikäinen. Deep learning for generic object detection: A survey. *International Journal of Computer Vision*, 128(2):261–318, 2020.

[26] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Attribute-based signatures. In Aggelos Kiayias, editor, *Topics in Cryptology – CT-RSA 2011*, pages 376–392, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[27] Avradip Mandal and Arnab Roy. Relational hash. Cryptology ePrint Archive, Report 2014/394, 2014. `https://ia.cr/2014/394`.

[28] S. Medasani, N. Srinivasa, and Y. Owechko. Active learning system for object fingerprinting. In *2004 IEEE International Joint Conference on Neural Networks (IEEE Cat. No.04CH37541)*, volume 1, pages 345–350, 2004.

[29] Hokey Min. Blockchain technology for enhancing supply chain resilience. *Business Horizons*, 62(1):35–45, 2019.

[30] Noam Nisan and David Zuckerman. Randomness is linear in space. 52(1):43–52, feb 1996.

[31] Corporate Nist. The digital signature standard. *Commun. ACM*, 35(7):36–40, 1992.

[32] OECD/EUIPO. *Global Trade in Fakes: A Worrying Threat*. Illicit Trade. OECD Publishing, Paris, 2021.

[33] Ravikanth Srinivasa Pappu. *Physical one-way functions*. PhD thesis, Massachusetts Institute of Technology, School of Architecture and Planning, Program in Media Arts and Sciences, 2001.

[34] Michael O Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical report, Massachusetts Inst of Tech Cambridge Lab for Computer Science, 1979.

[35] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[36] Alexey M. Romanov and Maria A. Volkova. The algorithm for classification and determination of the spatial position of moving objects. In *2019 IEEE EIConRus*, pages 657–660, 2019.

[37] Takami Sato, Junjie Shen, Ningfei Wang, Yunhan Jia, Xue Lin, and Qi Alfred Chen. Dirty road can attack: Security of deep learning based automated lane centering under physical-world attack. In *30th USENIX Security Symposium*, pages 3309–3326. USENIX Association, August 2021.

[38] Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In *Conference on the Theory and Application of Cryptology*, pages 239–252. Springer, 1989.

[39] Kenta Takahashi, Takahiro Matsuda, Takao Murakami, Goichiro Hanaoka, and Masakatsu Nishigaki. Signature schemes with a fuzzy private key. Cryptology ePrint Archive, Report 2017/1188, 2017. `https://ia.cr/2017/1188`.

[40] André Weil. Sur les fonctions algébriquesa corps de constantes fini. *CR Acad. Sci. Paris*, 210(592-594):149, 1940.

[41] Zachary Williams, Jason E Lueg, and Stephen A LeMay. Supply chain security: an overview and research agenda. *The International Journal of Logistics Management*, 2008.

[42] Guomin Yang, Duncan S. Wong, Xiaotie Deng, and Huaxiong Wang. Anonymous signature schemes. Cryptology ePrint Archive, Report 2005/407, 2005. `https://ia.cr/2005/407`.

[43] Piyi Yang, Zhenfu Cao, and Xiaolei Dong. Fuzzy identity based signature. Cryptology ePrint Archive, Report 2008/002, 2008. `https://ia.cr/2008/002`.

[44] Zhengxia Zou, Zhenwei Shi, Yuhong Guo, and Jieping Ye. Object detection in 20 years: A survey. *arXiv preprint arXiv:1905.05055*, 2019.

[45] 内閣府 科学技術・イノベーション推進事務局. 戦略的イノベーション創造プログラム（sip）iot 社会に対応したサイバー・フィジカル・セキュリティ 研究開発計画.

# 発表文献

### 査読無し国内会議

i 林リウヤ，浅野泰輝， 林田淳一郎，松田隆宏，山田翔太，勝又秀一，坂井祐介，照屋唯紀，シュルツヤコブ，アッタラパドゥンナッタポン，花岡悟一郎，松浦幹太，松本勉．“モノの電子署名：物体に署名するための一検討”．2021 年コンピュータセキュリティシンポジウム (CSS2021) 予稿集，pp.740-747，3E1-1，オンライン，2021 年 10 月.

ii 林リウヤ，浅野泰輝， 林田淳一郎，松田隆宏，山田翔太，勝又秀一，坂井祐介，照屋唯紀，シュルツヤコブ，アッタラパドゥンナッタポン，花岡悟一郎，松浦幹太，松本勉．“モノの秘匿性を考慮した「モノの電子署名」”．2022 年暗号と情報セキュリティシンポジウム (SCIS2022) 予稿集，3A3-2, 大阪，2022 年 1 月.

iii 浅野泰輝，林リウヤ，林田淳一郎，松田隆宏，山田翔太，勝又秀一，坂井祐介，照屋唯紀，シュルツヤコブ，アッタラパドゥンナッタポン，花岡悟一郎，松浦幹太，松本勉．“「モノの電子署名」の複数物体への拡張”．2022 年暗号と情報セキュリティシンポジウム (SCIS2022) 予稿集，3A3-6, 大阪，2022 年 1 月.

### 受賞歴

i 優秀論文賞，2021 年コンピュータセキュリティシンポジウム (CSS2021)，一般社団法人 情報処理学会，2021 年 10 月.