モノの電子署名：物体に署名するための一検討

林 リウヤ[1,a)]　浅野 泰輝[1]　林田 淳一郎[1,2]　松田 隆宏[2]　山田 翔太[2]　勝又 秀一[2]　坂井 祐介[2]
照屋 唯紀[2]　シュルツ ヤコブ[2]　アッタラパドゥン ナッタポン[2]　花岡 悟一郎[2]　松浦 幹太[1]
松本 勉[2,3]

概要：従来の電子署名方式では，電子データでない物体に対して電子署名を作成することができない．そこで，物体への操作を暗号学的に定式化することで，任意の物体を対象として作成が可能な電子署名である「モノの電子署名」を提案する．物体への操作は，物体を加工して新たな物体を作り出す操作であるコマンドと，物体を加工することなく電子データに変換する操作であるセンシングの 2 つに分けられる．このうちセンシングは同じ物体からであっても実行されるたびに異なる電子データを返すが，それに左右されることなく物体に対する有効な電子署名を作成できる方式が構成可能である．本稿では，この方式が満たすべき安全性定義とそれを満たす構成を示す．また，その構成の安全性が基盤とする電子署名方式における選択文書攻撃に対する存在的偽造不可 (EUF-CMA) に帰着できることも示す．

キーワード：電子署名，サプライチェーン

Signature for Objects: Formalization, Security Definition, and Provably Secure Constructions

Ryuya Hayashi[1,a)]　Taiki Asano[1]　Junichiro Hayata[1,2]　Takahiro Matsuda[2]　Shota Yamada[2]
Shuichi Katsumata[2]　Yusuke Sakai[2]　Tadanori Teruya[2]　Jacob Schuldt[2]
Nuttapong Attrapadung[2]　Goichiro Hanaoka[2]　Kanta Matsuura[1]　Tsutomu Matsumoto[2,3]

Abstract: Digital signatures cannot be used for non-digital things because they are considered to be used only for digital messages. We suggest a new signature scheme called "Signature for Objects," which can sign real objects. In this scheme, we formalize operating objects. The operation can be divided into two parts. One is to manipulate objects to create new ones, called Command. The other is just to convert objects into digital data, called Sensing. Even if the Sensing operation can return different data when it takes as input the same object, we can independently create a valid signature every time. In this paper, we define the security of this scheme and show one simple construction way to satisfy it. Moreover, we prove that it satisfies the security only by assuming that there exists a digital signature scheme satisfying EUF-CMA.

Keywords: digital signature, supply chain

1. はじめに

1.1 背景と目的

本研究の背景．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

[1] 東京大学生産技術研究所
Institute of Industrial Science, the University of Tokyo
[2] 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology (AIST)
[3] 横浜国立大学大学院環境情報研究院
Faculty of Environment and Information Sciences, Yokohama National University
[a)] rhys@iis.u-tokyo.ac.jp

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．こうした背景もあり，実際にサプライチェーンの信頼を損ねるようなインシデントの報告が増加している．より具体的には，あらゆる機器や製品の偽造が急速に拡大している．OECD[*1]のレポート [17] 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一つである．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．

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．しかし，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] European Organization for Economic Cooperation and Development

1.2 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を証明可能な「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，さらに以下について議論を行う: (1) 物体の操作に関する暗号学的定式化，(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，(3) モノの電子署名の簡易実装．

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一つかセンシングの一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．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．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リクエストすることができ，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，署名をリクエスト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二つ与えられたときに，それぞれの電子データを得るときに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．本稿では，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．

モノの電子署名の簡易実装．本研究では，センシングとして物体を画像に変換することを想定し，Relation Function として画像分類器を用いることで，シンプルかつ限定的な状況下でモノの電子署名が実際に実装可能であることを示す．物体から画像への変換はアルゴリズムとしてコーディングすることはできないため，予め MNIST のデータセットを用意することで 10 種類の物体（数字）を識別することとする．なお，MNIST データセットを用いる理由については比較的容易に高精度なネットワークが実現可能で，本稿で想定する精度 100%の理想的な Relation Function に近づけるためである．本稿における実装の結果，署名サイズは約 338bytes となった．この点についての考察は五章にて行う．

1.3 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 [11]．Williams らがまとめたように [23]，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 [2], [14]．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．

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 [5]．その後，RSA 署名 [19]，Rabin 署名 [18]，ElGamal 署名 [6] 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 [8]．その後も，Schnorr 署名 [22]，DSA 署名 [16]，ECDSA 署名 [10]，BLS 署名 [4] 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，先述の通り通常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) といった攻撃者のモデルを仮定して議論を進めるが，現実の物体を考える際には「攻撃者が物体に対して切るなどの（場合によっては不可逆の）アクションを行う」状況が考えられるため，それをどう定式化するか，およびどこまでのアクションを攻撃者に許可するかという問題が課題となる．

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．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 [12], [24] や物体のクラスまで認識する物体認識の研究 [1], [9] 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 [13] 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 [20] など，追跡や同一性判定に関する研究も数多く存在する．

情報セキュリティの観点からみると，画像処理において Adversarial Example の存在が非常に脅威となっている．佐藤ら [21] によると，自動運転において「とまれ」の標識であるにも関わらず，Adversarial Attack のために「進め」と解釈される可能性は否定できない．だが，「とまれ」であることを保証する道路標識そのものの電子署名を何らかの形で機械が読み取れるようにすると，仮に画像分類器が

「進め」の標識であると誤って認識したとしても，電子署名の検証フェーズでエラーが発生するため，画像分類器の誤った出力を検知することが可能となる．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．

2. 基本となる電子署名方式

シンタックス． $\mathbb{M} = \{0,1\}^*$ をメッセージ空間とする．[*2] 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三つの確率的多項式時間アルゴリズムの組 (DS.KG, DS.Sign，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^λ 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 σ 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 σ 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：

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

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 を任意の確率的多項式時間アルゴリズム（PPTA）が実行可能な攻撃者とする．A の攻撃成功確率を Succ_A^S を

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

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 1. 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 Succ_A^S が無視できる確率であることである．すなわち $\mathrm{Succ}_A^S \leq \mathrm{negl}(\lambda)$ 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．

[*2] 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。

3. 定義：モノの電子署名

3.1 物体に対する操作の定式化

3.1.1 センシング・コマンドオラクル

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二つに分けられる．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，異なる二物体 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，引数には一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に見える．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，コマンドを次の二つの操作として考える：(i) $\mathbb{X}_m$ から物体を一つ選んで $\mathbb{X}$ 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：

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

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．

定義 2. 物体に対する操作は，物体を電子データに変換す

るセンシングと物体に手を加えて変化させるコマンドという二つの操作に分けられ，それぞれの操作はオラクルにアクセスする形で表現する．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表される．ただし ϵ は空文字列を表す．

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

特に，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．

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 3. 同一性判定オラクル isSame は二物体を対象として，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，二物体 x_i, x_j に対して，

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

3.1.2 Physically Enhanced Algorithm

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，次節以降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. $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ を持つ 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 $\mathbb{X}_m$ に関するセンシングオラクル Sensing およびコマンドオラクル $\mathsf{Command} \in \mathbb{C}$ にアクセス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 アルゴリズムを実行可能な攻撃者に対して，EUF-CMA 安全な（通常の）電子署名方式が必要である．そこで，そのような電子署名方式を以下で定義する．

定義 5. 定義 1 では，PPTA 攻撃者 A に対してゲームを定義したが，$(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA アルゴリズム A に対しても同様のゲームを考えることができる．そのような攻撃者に対して Succ_A^S が無視できる確率であるとき，電子署名方式は $(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ でパラメタライズされた PEA 攻撃者に対して EUF-CMA 安全であるという．

3.1.3 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二つの異なる出力 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 は二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 6. $\mathbb{X}$ を物体集合，$\mathbb{S}$ をセンシングオラクルの集合とする．二つの物体 $x_i, x_j \in \mathbb{X}$ 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 は以下の性質を持つ：

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

上記の Relation function の性質が成立するためには，異なる二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 (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．

3.2 モノの電子署名方式の安全性定義

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，システムごとに一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 Π は以下の三つの組の多項式時間アルゴリズム（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^λ 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 σ を出力する．
- $\mathsf{SfO.Ver}(pk, \boxed{x}, \sigma) \to 0/1$ ：署名 σ の検証アルゴリズ

ム．物体 x を対象に，検証鍵 pk と署名 σ 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：

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

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 λ 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 λ 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 を定義をする．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，新しく三つのオラクル $\mathsf{Adv.Sign}(sk, \cdot)$, $\mathsf{Adv.Sensing}(\cdot)$, $\mathsf{Adv.Command}(\cdot)$ を考える．これら三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}, σ_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 6 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．以下の三つの動作を実行できる．(i) 一つは，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) 一つは，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) 一つは，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 σ_A の組を出力する．

A の勝利条件は l_{x_A} および $D_A \leftarrow \mathsf{Adv.Sensing}(l_{x_A})$ 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 7. 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 Succ^O_A とする．モノの電子署名方式 $\Pi = (\mathsf{SfO.KG}, \mathsf{SfO.Sign}, \mathsf{SfO.Ver})$ が EUF-COA を満たすとは，$(\mathbb{X}_m, \mathbb{C}, \mathsf{Sensing})$ を持つ任意の PEA 攻撃者 A に対して Succ^O_A が無視できる確率であることである．すなわち $\mathrm{Succ}^O_A \leq \mathrm{negl}(\lambda)$ 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．

4. 証明可能安全な構成

この章では前章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 $\Sigma_S = (\mathsf{DS.KG}, \mathsf{DS.Sign}, \mathsf{DS.Ver})$ 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 6 の Relation Function

とする．また，物体集合 $\mathbb{X}_T$ に属する物体に対して，与えられた $\mathsf{Sensing}(\boxed{\cdot})$ は次の性質を満たすとする：

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

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．

定理 1. 通常の電子署名方式 Σ_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 5 の EUF-CMA 安全性を持つならば，上の提案方式 Π_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 7 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 Π_1 に対する攻撃者とし，その攻撃成功確率を Succ^O_A とする．この A を用いて従来の署名方式に対する攻撃者 A' を構成する．ただし A' 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．A' の攻撃成功確率 $\mathrm{Succ}^S_{A'}$ は次のように定義できる：

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

ただし $\mathcal{M}$ は A' 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．

A' 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）：

$A'(pk)$
run $A(pk)$
when A queries l_x to $\mathsf{Adv.Command}(\cdot)$
(i.e. A does $\mathsf{Command} \in \mathbb{C}$ to $x \in \mathbb{X}_A$),
compute $\epsilon \leftarrow \mathsf{Command}(\boxed{x})$
add the new object to $\mathbb{X}_A$
when A queries l_x to $\mathsf{Adv.Sensing}(\cdot)$
(i.e. A asks a digital data for $x \in \mathbb{X}_A$),
compute $D \leftarrow \mathsf{Sensing}(\boxed{x})$
return D to A
when A queries l_{x_i} to $\mathsf{Adv.Sign}(sk, \cdot)$
(i.e. A asks a signature for $x_i \in \mathbb{X}_A$),
compute $D_i \leftarrow \mathsf{Sensing}(\boxed{x_i})$
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 A' 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，

$$\mathrm{Succ}^O_A \leq \mathrm{Succ}^S_{A'} \leq \mathrm{negl}(\lambda)$$

□

5. 概念実証 (Proof of Concept)

ここでは提案方式の概念実証を行う．本稿の実装においては，従来の署名方式 DS として BLS 署名 [4] を，また，最低限の実装のためシンプルかつ画像分類器の作成が比較的容易な MNIST のデータセット [7] を定義 6 の R として使ったモデルを想定する．なお，BLS 署名を用いる理由として，同じ安全性レベルを持つ RSA 署名などに比べて署名長が短い点 [3]，および既に C++で実装されている高速なペアリング計算ライブラリ mcl [15] が存在する点があげられる．提案方式との対応関係は，物体集合 $\mathbb{X}$ は 0 から 9 までの数字，Sensing は数字を手で書き画像にすること，R は二つの画像データ D, D' をそれぞれ画像分類器に入力して同一の分類結果となるか判定することである．

実装環境と設定． BLS 署名の実行には mcl [15] を用いた．使用した曲線は BN254 である．MNIST のネットワークとして 16，16，32，32，64，64，10 の 6 層からなる畳み込みニューラルネットワークを作成し，これを Python 言語で実装した．使用した計算機は CPU：AMD Ryzen 5 3600 CPU@3.60GHz × 6, OS : Kali GNU / Linux Rolling 64bit, RAM：8GB, C++ : version Debian 9.3.0-22, g++：version Debian 9.3.0-22，Python3 : version 3.9.2 である．

結果および考察． 実装したプログラムについて，画像分類の精度，署名生成と署名検証および R の計算にかかった時間，そして出力の大きさを計測し，概念実証および提案方式の性能について評価および考察を行う．特に，電子署名方式と R の計算がどのような性能を示すかに注目し，実用可能性について考察する．

表 1　モノの電子署名の実装結果

Table 1　The result of implementation for “Signature for Objects”

Image Classification Accuracy	99.34%
Sign	113 microsec
Verify (Pairing)	555 microsec
Verify (Image Classify)	433771 microsec
Signature Size $(D, \hat{\sigma})$	about 338 bytes

結果を表 1 に示す．まず，検証時の画像分類にかかる時間が署名およびペアリング演算と比較して 1000 倍ほど遅い点である．これについては，署名やペアリング演算が C++，画像分類が Python で行われているために発生していると考えられる．しかし，精度を維持したまま畳み込みニューラルネットワークを C++に移植する点も含め，本稿ではより汎用的なアプリケーションへの拡張，高速化，精度向上に関しては深く言及しない．

また，署名サイズについては，画像データに相当する D が約 300bytes である[*3]一方で，DS.Sign により生成される $\hat{\sigma}$ のサイズは 38bytes で固定である．提案方式を実システムへ応用する際には少なくともこの概念実証よりも複雑な物体や操作を取り扱うこととなり，R の計算への入力 D のサイズもより大きくなるため，一般の画像データに対する $\hat{\sigma}$ の割合はさらに小さいものとなることが予想される．さらに，概念実証で使用した BLS 署名は標準的な安全性を持ち，十分に性能が良い高速な実装が存在するので，既存システムへの機能追加によりモノの電子署名を実現するのは容易であると言える．

謝辞　本研究の一部は，JSPS 科研費 17KT0081 の助成を受けた．

参考文献

[1] Bansal, M., Kumar, M. and Kumar, M.: 2D Object recognition techniques: state-of-the-art work, *Archives of Computational Methods in Engineering*, pp. 1–15 (2020).

[2] Baryannis, G., Dani, S. and Antoniou, G.: Predicting supply chain risks using machine learning: The trade-off between performance and interpretability, *Future Generation Computer Systems*, Vol. 101, pp. 993–1004 (2019).

[3] Boneh, D., Gorbunov, S., Wahby, R. S., Wee, H. and Zhang, Z.: BLS Signatures, Internet-Draft draft-irtf-cfrg-bls-signature-04, Internet Engineering Task Force (2020). Work in Progress.

[4] Boneh, D., Lynn, B. and Shacham, H.: Short signatures from the Weil pairing, *International Conference on the Theory and Application of Cryptology and Information security*, Springer, pp. 514–532 (2001).

[5] Diffie, W. and Hellman, M.: New directions in cryptography, *IEEE Trans. Information Theory*, Vol. 22, No. 6, pp. 644–654 (1976).

[6] ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Information Theory*, Vol. 31, No. 4, pp. 469–472 (1985).

[7] Gangaputra, S.: Handwritten digit database (2013).

[8] Goldwasser, S., Micali, S. and Rivest, R. L.: A digital signature scheme secure against adaptive chosen-message attacks, *SIAM Journal on Computing*, Vol. 17, No. 2, pp. 281–308 (1988).

[9] Guo, Y., Bennamoun, M., Sohel, F., Lu, M. and Wan, J.: 3D object recognition in cluttered scenes with local surface features: A survey, *IEEE TPAMI*, Vol. 36, No. 11, pp. 2270–2287 (2014).

[10] Johnson, D., Menezes, A. and Vanstone, S.: The elliptic curve digital signature algorithm (ECDSA), *International journal of information security*, Vol. 1, No. 1, pp. 36–63 (2001).

[11] Lee, H. L. and Whang, S.: Higher supply chain security with lower cost: Lessons from total quality management, *International Journal of Production Economics*, Vol. 96, No. 3, pp. 289–300 (2005).

[12] Liu, L., Ouyang, W., Wang, X., Fieguth, P., Chen, J., Liu, X. and Pietikäinen, M.: Deep learning for generic object detection: A survey, *International Journal of Computer Vision*, Vol. 128, No. 2, pp. 261–318 (2020).

[13] Medasani, S., Srinivasa, N. and Owechko, Y.: Active Learning System for Object Fingerprinting, *2004 IEEE International Joint Conference on Neural Networks (IEEE Cat. No.04CH37541)*, Vol. 1, pp. 345–350 (2004).

[14] Min, H.: Blockchain technology for enhancing supply chain resilience, *Business Horizons*, Vol. 62, No. 1, pp. 35–45 (2019).

[15] Mitsunari, S.: `https://github.com/herumi/mcl`.

[16] Nist, C.: The digital signature standard, *Commun. ACM*, Vol. 35, No. 7, pp. 36–40 (1992).

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

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

[19] Rivest, R. L., Shamir, A. and Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, Vol. 21, No. 2, pp. 120–126 (1978).

[20] Romanov, A. M. and Volkova, M. A.: The Algorithm for Classification and Determination of the Spatial Position of Moving Objects, *2019 IEEE EIConRus*, pp. 657–660 (2019).

[21] Sato, T., Shen, J., Wang, N., Jia, Y., Lin, X. and Chen, Q. A.: Dirty Road Can Attack: Security of Deep Learning based Automated Lane Centering under Physical-World Attack, *30th USENIX Security Symposium*, USENIX Association, pp. 3309–3326 (2021).

[22] Schnorr, C.-P.: Efficient identification and signatures for smart cards, *Conference on the Theory and Application of Cryptology*, Springer, pp. 239–252 (1989).

[23] Williams, Z., Lueg, J. E. and LeMay, S. A.: Supply chain security: an overview and research agenda, *The International Journal of Logistics Management* (2008).

[24] Zou, Z., Shi, Z., Guo, Y. and Ye, J.: Object detection in 20 years: A survey, *arXiv preprint arXiv:1905.05055* (2019).

[*3] 本実装においては画像データのサイズに大きなばらつきは存在しないが，本来センシングの出力サイズに関する制約を仮定していないことに注意されたい．