Vol.2021-SPT-41 No.15
2021/3/1

暗号技術の等価的な物理的モデル化検討

石島 慧[1,a)]　金岡 晃[1,b)]

概要：情報社会の現代において暗号技術の高度化が進んでいる中、高度化を果たすために利用される技術も複雑化している。一方、暗号を専門としていない技術者が暗号技術を使う際に、適切に利用できずに危険な状態のまま実装や利用してしまうことがこれまでの研究により明らかになっている。本研究ではわかりやすい表現や直感的な例を用いて技術者に暗号技術について理解を促すことを目的とし、そのためのアプローチの 1 つとして暗号技術の等価的物理モデリングの実現方法を検討する。等価的物理モデリングの検討に先立ち、用語の定義や評価基準の検討を行う。その後等価的物理モデリングの例を 4 種類提案し、それらを既存の物理モデリング手法と合わせて評価をし、その等価性を議論し、等価性が満たされない要素に関しての共通性に関して考察する。

Equivalent physical modeling of cryptographic technique

1. はじめに

高機能暗号に代表される暗号技術は、高い機能性や安全性を提供する一方で、利用される技術や数学は複雑化してきている。一方で、暗号理論を専門としていない技術者が暗号技術を利用するにあたり、適切な利用ができず危険な状態のまま実装や利用をしてしまうことがこれまでの研究により明らかになっている。これまでの研究によりわかってきた暗号技術の誤使用の実態は、高機能な暗号技術ではなく RSA 暗号や AES などすでに広く利用されている暗号技術において発生していることが報告されており、技術が複雑化している高機能な暗号技術においては誤使用はより深刻な問題となることが懸念される。

複雑化した暗号技術の誤使用に対するアプローチとして、暗号技術の理解が少なくとも適切に暗号技術を利用できるように開発シーンにおいて自動化・や半自動化（支援）を行う技術の研究開発がある。もう 1 つのアプローチとして、適切な利用ができるように技術の理解に導く方法がある。そこでは API の提供と API 利用法の丁寧かつ充実した説明、チュートリアルの準備、充実したサンプルコードの準備などの必要性が示されてきていた。本研究では、もう 1 つのアプローチとして暗号技術を適切に理解してもらうことに焦点を当てる。

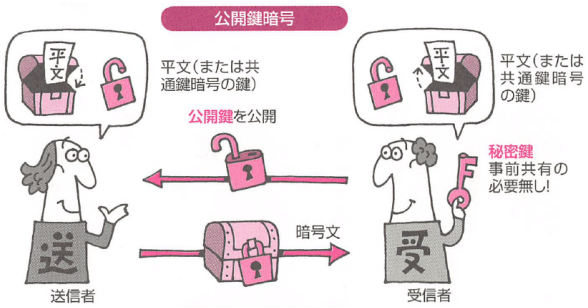


図 1: 公開鍵暗号方式解説に比喩として南京錠が採用されている例（”トコトンやさしい暗号の本”[1] P.58 の図）

複雑な技術を理解する手段の 1 つとして比喩を用いた解説がある。たとえば公開鍵暗号方式を用いた暗号化（Encryption）と復号（Decryption）では南京錠が比喩として使われることがある（図 1）。比喩は対象となる事象などを共通の要素をもつ他の物事や事象に置き換えて表現する方法であり、文章やスピーチなどに利用される。本論文では、こういった置き換えを文章やスピーチにとどまらずに拡張して考え、モデリングと呼ぶこととする。近年の技術の発達により、モデリングは文章やスピーチなどの文字によるものにとどまらず、図表を使った例や、物理的な例を実際に用意し、それらを画像や動画としてメディアにすることが可能になった。本研究ではこの中でも物理的な例を実際に用意するモデリングに着目する。

[1] 東邦大学
Toho University, Funabashi, Chiba 274–8510, Japan
[a)] 5517006i@st.toho-u.jp
[b)] akira.kanaoka@is.sci.toho-u.ac.jp

南京錠の例は公開鍵暗号の性質理解に一定の効果があると考えられるが、利用されるモデリングによっては暗号技術の行為への理解はされるが、暗号として成り立つための安全性などの理解の助けにならない手法となることがある。その結果暗号技術が誤って理解され、適切でない利用を促進してしまうリスクが存在する。

そこで本研究では以下を Research Question と置いた。

RQ: 暗号の誤使用に対して、暗号プロトコルの処理に加え、安全性の根拠や暗号技術の特性（秘匿性・機密性、完全性）を適切に表現する物理的モデリングが考えられないだろうか？

この Research Question に答えるために、本研究ではまず適切な表現を行うモデリングを等価的であると表現し、その定義を行う。次に等価的物理モデリングの評価方法と基準について議論する。その後、いくつかの物理モデリングを提案し、その等価性の評価を行い、従来のモデリングや提案モデリングに共通する特徴を議論する。

提案した物理モデリングと過去に行われた物理モデリング事例に対し評価を行った結果、RSA 暗号における素因数分解問題の困難性、DH 鍵交換における離散対数問題の困難性の再現がいずれも達成されなかったことが示された。これらのことから、物理モデリングの等価性において、暗号アルゴリズムの安全性根拠となる数学的困難性のモデリングの難しさが明らかになった。これらの詳細について 2 章以降で示していく。

2. 関連研究

2.1 暗号 API の誤使用

2.1.1 誤使用の調査

2013 年、Egele らにより、暗号 API の適切利用がソフトウェア開発者にとって容易ではないことが議論された [2]。Egele らは Android アプリケーションにおける暗号 API の誤使用があることに着目し、その誤使用の解析を行う軽量手法を提案した。そこで解析対象とされている項目は、共通鍵暗号における ECB 利用の有無や CBC モードにおける非ランダムな初期ベクトル（IV）利用の有無など共通鍵のモードに関する話や、固定の暗号鍵利用、パスワードにおける Salt 値の固定利用、ストレッチング（繰り返し）の回数の少なさ、乱数生成時の関数利用での適切な Seed 値の利用であった。

Egele らの研究は、暗号技術を研究するものにとっては初歩的とも思えるものである。しかし一方でそれらのチェックが有効に効くことが示されており、逆説的に実際のアプリケーション開発の現場における誤使用の発生ポイントと暗号研究者の認識とのギャップを強く示すものになったと言える。なお、これらのチェックリストで最も多く該当したものが、ECB モードの利用であった。これは調査時において BouncyCastle で default になっていたことが原因である可能性が指摘されている。

その後、2014 年になり Lazar による調査や [3]、Li らによる暗号 API の追跡手法の提案があった [4]。Lazar らによる調査は、2011 年から 2014 年にかけて明らかになった暗号関連の脆弱性 269 件を調査し、その結果 83%が暗号の誤使用であることが明らかにされた。Li らは、iOS のアプリケーションをターゲットにし、静的解析と動的解析を組み合わせて暗号 API の利用を追跡する iCryptoTracer を提案した。そして提案システムにより調査対象の 98 のアプリのうち 64 のアプリで暗号の誤使用を発見した。それらの誤使用のターゲットは固定の鍵の利用、CBC 用に非ランダムな IV が使われているか、そして Stateless な暗号が利用されていないか、というものであり、Egele らの研究と同様、暗号技術の種類としては広範に利用されている暗号の一部分がターゲットになっていた。

2015 年に発表された Chatzikonstantinou らの論文は、暗号の誤使用の調査ターゲットを大きく広げた [5]。まずターゲットを大きく「Weak Cryptography (C)」「Weak Implementation （I)」「Weak Key (K)」「Weak Cryptographic Parameters (P)」と 4 つに分類した。そしてそれぞれの分類でさらに項目が細分化されている。分類 C では 6 項目、I で 6 項目、K で 4 項目、P で 8 項目となっている。これらの項目は Egele らが挙げた項目を包含するものとなっている。新たに取り上げられた項目の一例をあげると、分類 C では MD5 といったアルゴリズムの利用や暗号学的に安全ではない疑似乱数発生器の利用、分類 I では標準アルゴリズムの再実装や OAEP ではない RSA 暗号の利用などが入っている。K では鍵サイズやハードコードされた鍵についての項目があり、P では主に共通鍵のモードや IV に関する項目が並んでいる。

2.2 誤使用の原因把握

なぜ開発者がそういった誤使用をしてしまうかという人間的な視点で調査が複数行われている。

Acar らは、まずポジションペーパーとして断片的に語られてきた開発者が誤使用する原因について、統合的に扱うべく調査が必要だと示した [6]。Acar らはそのポジションペーパーに先立ち、IEEE SP で Android アプリケーションを脆弱に作ってしまう原因を探るべく、開発者が開発時の得る情報源に着目し、異なる情報源を与えた場合での脆弱性の発生について調査をしていた [7]。この論文は暗号の誤使用だけに着目したものではなく、Android アプリケーションでソースコードに起因する脆弱性について調査したものであった。その結果、多くの開発者はオープンな開発者フォーラムである StackOverflow を利用した場合には動作するアプリケーションが作成可能であるが脆弱なアプリケーションになる傾向があり、公式なドキュメントを参考に開発をした開発者は脆弱なアプリケーションは作らない

もののきちんとした動作ができないアプリケーションになる傾向があることが示され、公式なドキュメントのユーザビリティ向上が必要であることを主張した。

2.3 誤使用への対策

誤使用の原因把握と並行するように、対策手法の研究も進みつつある。

暗号 API の誤使用に対して修正を図るアプローチは、2015 年に Arzt らによって Eclipse のプラグインとして提案がされた [15]。対象言語を Java に限定し、開発中のソースコードの分析を行うアプローチであった。当初は OpenCCE とプロジェクト名を付けていたが、その後 CogniCrypt とプロジェクトが変わり、現在でも開発が行われている [16]。Arzt らの論文では提案だけにとどまっており、実際の評価までは至っていなかった。

2016 年になり、Ma らが CDRep を提案した [17]。Arzt らと同じく、暗号の誤用を自動修復するツールであり、Android や iOS のアプリケーションを対象にしている。修正パターンはヒューリスティックに準備がされており、誤用の分類は 7 種類としていた。この分類は Egele らの研究を踏襲するものであり、共通鍵の利用がが主なターゲットとなっている。ツールの評価では、1262 件のうち 95%の修復に成功したとしている。

暗号 API の誤使用だけではなく、より広く脆弱性全般もターゲットにした動きとして、Nguyen らの研究がある [18]。こちらも統合開発環境にプラグインを導入することで実現するものであり、開発者が陥りがちな 13 の項目を調査対象としている。特徴的なこととして、教育視点としてチュートリアルのようなテストプロジェクトが用意されている。

3. 既存の暗号技術モデリング事例

3.1 動画による DH の解説

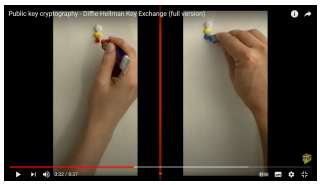
YouTube チャンネル Art of the Problem で絵の具を用いた DH の解説動画 [20] が公開されている。これは DH における G や a、b というパラメータを絵の具、パラメータを用いた演算を混ぜる動作に置き換えたものである。

図 2-(a) のように DH における共有する素数 G として白と黄色の絵の具を用意し、乱数 a として赤色の絵の具、乱数 b として青色の絵の具を用意している。

a 乗または b 乗して P を法とした剰余演算を行う部分を絵の具を混ぜることに置き換えている。それぞれ求めた $G^a \bmod P$、$G^b \bmod P$ が図 2-(b) の状態である。

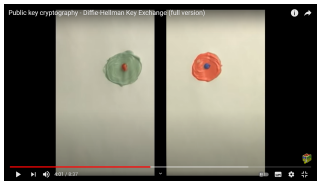
次にそれぞれ求めた数を表す紙を交換し、その交換した数に対して a 乗または b 乗を意味する絵の具を混ぜることで P を法とした剰余演算を行うことを示している。これを図 2-(c) に示した。

最後に、図 2-(d) の通りそれぞれが $(G^b \bmod P)^a \bmod P$、



(a) G、a、b に対応する絵の具を用意（3 分 32 秒付近）

(b) $G^a \bmod P$、$G^b \bmod P$ に対応する混ぜた絵の具（3 分 41 秒付近）



(c) $(G^b \bmod P)^a \bmod P$、$(G^a \bmod P)^b \bmod P$ の準備（4 分 1 秒付近）

(d) $G^{ab} \bmod P$ の共有に対応する混ぜた絵の具（4 分 6 秒付近）

図 2: ”Public key cryptography - Diffie-Hellman Key Exchange (full version)”[20] のスクリーンショット。時間情報は動画再生位置を示す

$(G^a \bmod P)^b \bmod P$ を計算に相当する絵の具を混ぜる作業を行い共通する $G^{ab} \bmod P$ を手に入れる。双方が同じ色に混ざっていることで鍵の共有ができたことを視覚的に理解させることを狙ったものであることが考えられる。

3.2 文章による暗号化（Encryption）の比喩

修辞技法の 1 つである比喩は、対象となる事象などを共通の要素をもつ他の物事や事象に置き換えて表現する方法である。技術用語を比喩を用いて理解の促進を図るアプローチは多く行われている。たとえば Google のシンクタンクである jigsaw が The Washington Post とともに立ち上げたプラットフォーム「Sideways Dictionary」では、比喩を使ってテクノロジー用語を解説している [19]。

その用語の 1 つに Encryption があり、いくつかの比喩が紹介されている。その中の 1 つに”It’s like wearing clothes.” がある。服を着ることで人の裸が隠れることを Encryption の比喩として用いたものである。

4. 等価的物理モデリング

4.1 物理モデルと物理モデリング

比喩では文章やスピーチなど置き換える対象が文字や言葉であることが基本であるが、インターネットの広まりや静止画と動画コンテンツの利活用の容易さ向上により、置き換える対象が図や動画とすることが可能となった。さらに発展して考えると、何か共通の要素を持つ他の物理的な事象に置き換え、その物理的な事象を実際に用意しそれを直接ユーザに見せることや動画や写真等で撮影するなど

してメディアを通して伝えることも可能になる。本論文では、そういった「対象となる事象を共通の要素を持つ物理的な事象に置き換えること」を物理モデリングと呼び、置き換えられたものを物理モデルと呼ぶこととする。

4.2 等価的物理モデリング

技術用語を物理モデルにより表現するにあたって、その技術が持つ機能を物理モデルが的確に表現されているかは非常に重要である。物理モデリングにより技術用語の理解に論理的な誤りが発生することは避けられなければならない。暗号技術の物理モデリングにおいては、暗号化や復号、署名や認証、一方向性などさまざまな機能を的確に表現するだけではなく、その機能が安全であることの根拠も併せて的確に表現されなければ、暗号技術の理解に誤りを生じさせる恐れがある。暗号技術の物理モデリングでは、この 2 点を求めることで有効な物理モデリングであると言うことができる。そこで本研究では、下記の 2 点を満たす物理モデリングを等価的物理モデリングと定義する。

- 暗号技術が持つ機能が的確に表現されている
- 暗号技術が持つ安全性の根拠が的確に表現されている

たとえば 3.2 で挙げた Sideways Dictionary における暗号化（Encryption）の比喩である”It’s like wearing clothes.”を共通鍵暗号の比喩として用いた場合は、平文は裸の人を表し、服を着ることが暗号化、服を脱ぐことが復号を示すこととなる。人と服といった物理的な事象に置き換えているため物理的なモデリングであると言えよう。また、暗号化の機能としてカプセル化を連想させる表現であるため機能の表現としては適切であると言える。一方で、一般的には第 3 者が着てる服を脱がすことは倫理的には避けられるべきであるが技術的には困難性は低いと言えるため、安全性の根拠が的確に表現されているとは言い難い。よって、本論文の定義に基づけばこの比喩は等価的な物理モデリングではない、となる。

5. 等価的物理モデリングの評価基準

検討した物理モデルが等価的か評価するためには基準が必要である。物理モデルを評価するにあたって評価基準はアルゴリズムに依らず統一された共通の基準が採用されることが望ましい。しかし、例えば物理モデリング対象が公開鍵暗号アルゴリズムと共通鍵暗号アルゴリズムでは両者の性質の違いから評価の基準を同一にすることは難しいことは容易に想像できる。むしろ基準を共通化しようとすれば評価項目を汎用的にせねばならず、その結果評価基準が曖昧になる恐れがある。したがって本論文では評価基準を共通する基準とアルゴリズムごとに設定される基準の 2 つに大別した。

- 共通評価基準：アルゴリズムの正確性、安全性の根拠の表現
- アルゴリズムごとの評価基準

6. 物理モデルの提案と評価

本研究では RSA 暗号について 1 種類、DH について 2 種類の物理モデルを検討した。大別すると視覚的な物理モデリングと味覚的な物理モデリングを試みたものの 2 種類になる。

6.1 フリクションペンを用いた RSA 暗号の視覚的物理モデル

6.1.1 フリクションペン

フリクションペンとは 60 ℃以上で消色しマイナス 10 ℃以下になると復色する性質 [21] を持つインキを用いたペンである。インキを消色させる手段として、ペンに付属しているラバーで擦る方法やドライヤーやアイロン等で温める方法がある。復色の手段として、冷蔵庫に入れて冷やす方法や冷却スプレーを使う方法などがある。

6.1.2 概要

RSA 暗号の平文をフリクションインキで書かれた物、暗号化時のべき乗剰余演算をフリクションインキの消色、復号時のべき乗剰余演算をフリクションインキの復色と置いて視覚的に物理モデリングを試みた。

6.1.3 手法

以下の手順をとる。

平文作成　フリクションペンを用いてなんらかを紙上に書く

暗号化　紙を温めて消色させる

復号　紙を冷やして復色させる

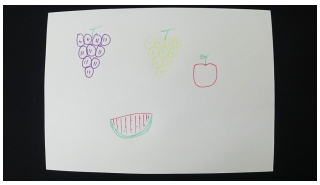
まず図 3-(a) に示すように紙とフリクションペンで平文となる文字や絵などを用意する。次にアイロンを用いて平文を温めることでインキを消色させる。この消色したものが図 3-(b) に示したように暗号文となる。最後に暗号文を冷却スプレーで冷やし、インキを復色させることで復号とする。これを図 3-(c) に示した。

6.1.4 評価基準に基づく評価

評価基準に基づいて著者ら自身により本提案モデル評価を行った。その結果を表 1 に示す。本モデルでは共通評価基準のみで評価を行った。

暗号化に用いる鍵と復号に用いる鍵が異なる非対称性があり公開鍵暗号アルゴリズムにおける重要な要素がモデリングされていると言える。また暗号文は第 3 者が見ても平文が予想できないことから暗号文としてモデリングがされているとも言える。一方で、復色させる手段はユーザを問わず「冷やす」で統一されていることから、ユーザごとに鍵が異なることが表現されていない。そのためアルゴリズムの正確性に対する評価は△とした。

RSA 暗号は素因数分解の困難性を用いて構成されているが、その困難性が表現されているとは言えない。そのた



(a) 平文に対応する絵

(b) 暗号文に対応する絵

(c) 復号された平文に対応する絵

図 3: フリクションペンを用いた RSA 暗号の視覚的物理化モデル

表 1: フリクションペンを用いた RSA 暗号化の視覚的物理モデルの評価

評価項目		判定
共通評価基準	アルゴリズムの正確性	△
	数学的な困難性の表現	×

め数学的な困難性の表現は×とした。

6.2 フリクションペンを用いた DH の視覚的物理モデル

6.2.1 概要

DH における G を紙、a と b を鍵交換を行うユーザがそれぞれ紙に書く文字や絵、べき乗剰余演算をインキの消色に置き換え視覚的に物理モデリングを試みた。

6.2.2 手法

公開パラメータの共有 G となる紙を 2 者間で共有する。

G^a または G^b の計算 鍵交換を行うユーザがそれぞれフリクションペンと紙を用いてなんらかを紙上に書く

$G^a \bmod P$ または $G^b \bmod P$ の計算 鍵交換を行うユーザがそれぞれ紙を温めて消色させる

$G^a \bmod P$ または $G^b \bmod P$ の送付 消色した紙を交換する

$(G^b \bmod P)^a$ または $(G^a \bmod P)^b$ を計算 鍵交換を行うユーザがそれぞれ交換した紙に「G^a または G^b の計算」実施時と同じものを紙上に書く

$(G^b \bmod P)^a \bmod P$ または $(G^a \bmod P)^b \bmod P$ を計算 鍵交換を行うユーザがそれぞれ紙を温めて消色させる

それぞれを図**??**に示す。

6.2.3 評価基準に基づく評価

評価基準に基づいて著者ら自身により本提案モデル評価を行った。その結果を表 2 に示す。本モデルでは共通評価基準のみで評価を行った。

$\bmod P$ を消色に用いることは公開パラメータを用いるため数学的な困難性の表現は×とした。

表 2: フリクションペンを用いた DH の視覚的物理モデルの評価表

評価項目		判定
共通評価基準	アルゴリズムの正確性	△
	数学的な困難性の表現	△

めユーザ間で共用可能であり、お互いがそれぞれの異なる情報を用いて処理をしている。また手順に復色が含まれないために、秘密情報によるべき乗剰余演算を行った結果からは相手の秘密情報はわからず、演算結果を交換している経路を盗聴（のぞき見）している第 3 者に対してもそれぞれの秘密情報はわからない。そのためアルゴリズムの手順に忠実なモデリングになっていると考えられる。一方で、本モデリングは交換手順の中に復色が含まれないため、最終的に交換された情報は紙に含まれる物質としては当初の紙（G）とは異なるものになっているが、視覚的には当初の紙と区別がつかないものとなっている。視覚的な等価的物理モデリングを標榜しているため、この点が解決されることが望ましい。そのためアルゴリズムの正確性に対する評価は△とした。

DH 鍵交換は離散対数問題の困難性を用いて構成されている。本モデルにおける離散対数問題の解決はフリクションインキの復色を行うこと同じであると言える。復色を行うためには 10 度以下に冷やす必要があり行為に一定の制約が伴うため困難性の表現として一定の評価はできるが、離散対数問題の困難性と同等であるとは言い難い。そのため数学的な困難性の表現は△とした。

6.3 コーヒー、ミルク、ガムシロップを用いた DH の味覚的物理モデル

6.3.1 概要

DH における G をコーヒーが入ったカップ、a をミルクの量、b をガムシロップの量とし、べき乗演算をミルクまたはガムシロップをカップに入れる行為、剰余演算をカップの中身を混ぜる行為に置き換え味覚的に物理モデリングを試みた。

6.3.2 手法

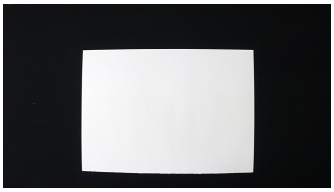
公開パラメータの共有 G となる同じ味のコーヒーをカップに入れ 2 者間で共有する

G^a または G^b の計算 鍵交換を行うユーザがそれぞれミルクまたはガムシロップをコーヒーに入れる

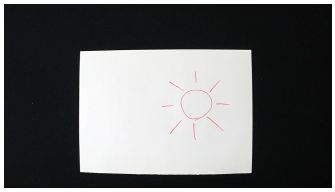
$G^a \bmod P$ または $G^b \bmod P$ の計算 鍵交換を行うユーザがそれぞれカップの中身を混ぜる

$G^a \bmod P$ または $G^b \bmod P$ の送付 それぞれのカップを交換する

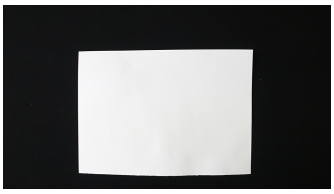
$(G^b \bmod P)^a$ または $(G^a \bmod P)^b$ を計算 鍵交換を行うユーザがそれぞれ交換したカップに「G^a または G^b の計算」実施時と同じ量のミルクまたはガムシロップを



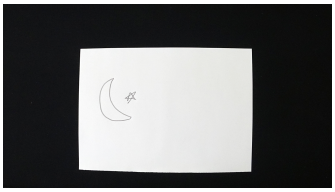
(a) G に対応する紙



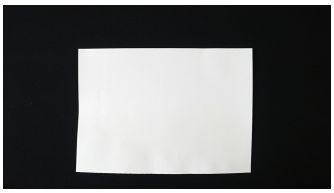
(b) G^A に対応する絵



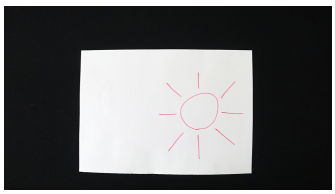
(c) $G^A modP$ に対応するインキが消色した状態の絵



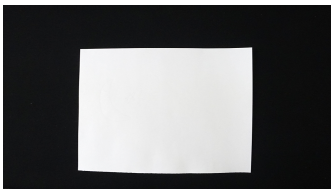
(d) G^B に対応する絵



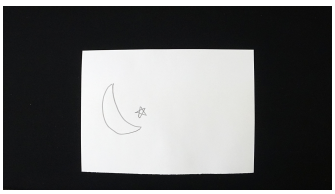
(e) $G^B modP$ に対応するインキが消色した状態の絵



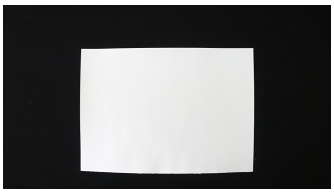
(f) $(G^B modP)^A$ に対応する絵



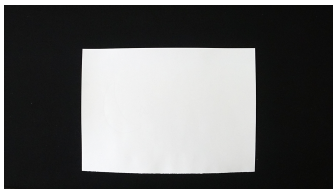
(g) $(G^B modP)^A modP$ に対応するインキが消色した状態の絵



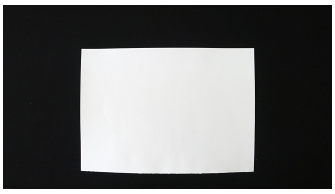
(h) $(G^A modP)^B$ に対応する絵



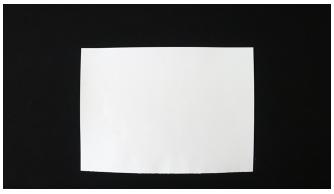
(i) $(G^A modP)^B modP$ に対応するインキが消色した状態の絵



(j) $(G^A modP)^B modP$ に対応するインキが消色した状態の絵



(k) $G^{A\times B} modP$ に対応するインキが消色した状態の絵



(l) $G^{A\times B} modP$ に対応するインキが消色した状態の絵を復色させたもの

入れる

$(G^b \bmod P)^a \bmod P$ または $(G^a \bmod P)^b \bmod P$ を計算
鍵交換を行うユーザがそれぞれカップの中身を混ぜる

6.3.3 評価基準に基づく評価

評価基準に基づいて著者ら自身により本提案モデル評価を行った。その結果を表**??**に示す。本モデルでは共通評価基準のみで評価を行った。

mod P を混ぜる行為に用いることは公開パラメータを用いるためユーザ間で共用可能であり、お互いがそれぞれの異なる情報を用いて処理をしている。最終的に交換されたコーヒーカップの中身の味は同じ味になり、交換は無事に成立している。そのためアルゴリズムの手順に従ったモデリングになっていると考えられる。そのためアルゴリズムの正確性に対する評価は○とした。

DH 鍵交換は離散対数問題の困難性を用いて構成されている。本モデルにおける離散対数問題の解決はカップの中身を味わったことによりミルクまたはガムシロップの量を正確に推定すること同じであると言える。量を正確に推定することは困難であると言える一方で、甘い/甘くないあるいはミルクの味がする/しないというそれぞれ 1 つの軸の上に連続で表現される情報であるため、近似の値の推定は容易である。そのため離散対数問題の困難性と同等であるとは言い難い。そのため数学的な困難性の表現は△とした。

表 3: コーヒー、ミルク、ガムシロップを用いた DH の味覚的物理モデルの評価表

評価項目		判定
共通評価基準	アルゴリズムの正確性	○
	数学的な困難性の表現	△

6.4 Art of the Problem らのモデルの評価

本節では既存の暗号技術モデリング事例で挙げた YouTube チャンネル Art of the Problem で絵の具を用いた DH の解説動画 [20] を提案手法と同様に評価する。

6.4.1 概要

DH における G を白と緑の絵の具、a と b をそれぞれ異なる絵の具、剰余演算を絵の具を混ぜる行為に置き換え視覚的に物理モデリングを試みたものと言える。

6.4.2 手法

公開パラメータの共有　G となる白と緑の絵の具を 2 者間で共有する

G^a または G^b の計算　鍵交換を行うユーザがそれぞれの絵の具を用意する

$G^a \bmod P$ または $G^b \bmod P$ の計算　鍵交換を行うユーザがそれぞれ絵の具を混ぜる

$G^a \bmod P$ または $G^b \bmod P$ の送付　それぞれの混ぜた絵の具を交換する

$(G^b \bmod P)^a$ または $(G^a \bmod P)^b$ を計算　鍵交換を行う

表 4: 絵の具を用いた DH の視覚的物理モデルの評価表

評価項目		判定
共通評価基準	アルゴリズムの正確性	△
	数学的な困難性の表現	△

ユーザがそれぞれ交換した絵の具に「G^a または G^b の計算」実施時と同じ量と色の絵の具を入れる
$(G^b \bmod P)^a \bmod P$ **または** $(G^a \bmod P)^b \bmod P$ **を計算**
鍵交換を行うユーザがそれぞれ絵の具を混ぜる

6.4.3 評価基準に基づく評価

評価基準に基づいて著者らにより本提案モデル評価を行った。その結果を表 4 に示す。本モデルでは共通評価基準のみで評価を行った。

mod P を混ぜる行為に用いることは公開パラメータを用いるためユーザ間で共用可能であり、お互いがそれぞれの異なる情報を用いて処理をしている。最終的に交換された絵の具の中身の味は同じ味になり、交換は無事に成立している。一方で、G を白と緑の 2 色の絵の具として置き換えており、それぞれのユーザの情報 a と b も同じく絵の具としている。混ぜる行為をべき乗剰余演算と考えると、白と緑の混ぜる行為が G にはならず、矛盾が生じてしまうなど、べき乗に当たる行為がモデルに的確に反映されているとは言い難い。そのためアルゴリズムの正確性に対する評価は△とした。

DH 鍵交換は離散対数問題の困難性を用いて構成されている。本モデルにおける離散対数問題の解決は混ぜた色を見たことにより白と緑以外の 2 色のどちらかの色を正確に推定すること同じであると言える。ユーザが選択できる色の種類によっては色を正確に推定することが困難となる言える一方で、色の三原色（Yellow、Magenta、Cyan）としてそれぞれの色がどの色から成立するかの知見はすでに多く容易に得られるものになっていることに加え、混ぜた色の度合いは三原色をそれぞれ 1 つの軸として連続で表現される情報であるため、近似の値の推定は容易である。そのため離散対数問題の困難性と同等であるとは言い難い。そのため数学的な困難性の表現は△とした。

7. 考察と課題

本論文は暗号技術を適切に表現する物理モデルの実現に向けた検討をしているが、提案した等価的物理モデリングの定義やいくつかの物理モデリング手法は実現を達成したとは言い難い。特に提案物理モデリング手法はいずれもどこかに適切な表現とは言い難い部分が残るものとなっており、より深い検討と違うアイデアが求められることが示された。

本章では、本論文による検討により得られた知見を整理し、実現に向けた今後の課題を明らかにすることを狙う。

7.1 暗号技術の安全性表現の難しさ

本論文では RSA 暗号の視覚的物理モデリング 1 種類、DH 鍵交換の視覚的物理モデリングと味覚的物理モデリングをそれぞれ 1 種類ずつ、計 3 種類を提案した。また既存のモデリングとして絵の具を用いた DH 鍵交換の例と、暗号化（Encryption）の比喩の例を挙げた。

これらの 5 つのモデリングはいずれも等価的物理モデリングとは言えないものであったが、等価性を評価するにあたり共通点があることがわかる。いずれも暗号技術として重要な安全性の根拠について的確なモデリングがされていなかった。比喩などの修辞表現や物理的なモデリングを検討するにあたり、手順などを置き換えることは一定の成功を果たしている一方で安全性の根拠についてのモデリングに成功したとは言い難く、等価的なモデリングを果たすにはこの 2 点が重要であることがあらためて明らかになったと考えられる。

7.2 等価性議論の基準明確化

等価性を議論するにあたり「的確」や「安全性」をキーワードとしていたが、この的確さや安全性は評価者や評価する対象、そして物理モデリングがどう利用されるかによって大きく異なることが良そうされる。たとえば、エンドユーザにとって安全性の根拠の理解よりも手順として理解してもらうことが重要であるかもしれない。一方で、ソフトウェア開発者などは開発において利用する暗号技術の安全性の理解は十分にしておくべきであることから、モデリングとしては手順と同等あるいはそれ以上に安全性理解が必要とされるかもしれない。

公開鍵暗号の研究において安全性となると一方向性や強秘匿性、頑強性をもとにその解読難易度を IND-CCA 安全などさまざまな定義がされている一方で、それらの安全性は暗号技術の開発者にとって必要な知識であり、暗号技術の開発者以外のユーザにとっては「暗号文から鍵を推測されないこと」といった単純化された安全性の理解で十分である可能性は十分ある。ユーザごとに暗号技術に対して求められるリテラシが異なることから、必要とされる理解度は 1 つに定まらないことは自然であると言える。このことから、等価的物理モデリングを検討ためには、まず対象のユーザの設定とそのユーザに求める暗号技術のリテラシの設定がされることが必要であることがわかる。

本論文において、等価性の評価基準として共通評価基準とアルゴリズムごとの評価基準と分けて提案をしたが、論文中で提案したモデリングと言及した既存モデリングの評価においてはアルゴリズムごとの評価基準は利用しなかった。本論文で提案あるいは紹介したモデルは公開鍵暗号技術がほとんどであり、さらに古典的な公開鍵暗号技術であった。モデリングの対象が共通鍵暗号系のブロック暗号やストリーム暗号、ブロック暗号の利用モードとなるケー

スや、暗号学的ハッシュ関数となるケースもある。この場合、それらの暗号技術に応じた評価基準が求められることは自然である。さらには高機能暗号技術をモデリングするとなると、その技術に応じた特殊な条件を検討する必要性が出てくることは容易に想像できる。そのためこれらは等価的物理モデリングを今後さらに発展させるためには必要であると考える。

7.3 物理的な現象の理解と整理

たとえば素因数分解問題や離散対数問題の物理的モデリングを考えた場合、重要になるのはそれに近い物理現象を見つけ出しモデリングに採用することとなる。本論文で挙げた特殊なインキや絵の具の混色、味の変化などは素因数分解や離散対数問題の物理的モデリングとしては近い物理現象とは言い難い。まずは世の中に存在するさまざまな物理現象を暗号技術の物理的モデリングの視点で俯瞰し、整理することが今後の課題となるだろう。一方で、実在する物理的な現象であってもモデルを体感するユーザにとって身近あるいは理解が容易な物理現象でなければ、その現象理解自体に困難性が伴ってしまうために、等価的物理モデリングの実現は難しくなるだろう。その点に注意した整理が期待される。

8. まとめ

本論文では、わかりやすい表現や直感的な例を用いて技術者に暗号技術について理解を促すことを目的とし、そのためのアプローチの 1 つとして暗号技術の等価的物理モデリングの実現方法を検討した。等価的物理モデリングの実現に先立ち、物理モデリングや等価的の定義を行い、等価的物理モデリングの評価基準を議論した。そして 3 種類の物理モデリングを提案し、その等価性を評価した。評価にあたり既存モデリング手法も 1 つ評価を行った。評価の結果、暗号技術の手順についてはモデリングにより適切な表現となっている例があったものの、いずれのモデリングにおいても暗号技術の安全性の根拠を適切に表現していると評価されるものがなかった。そのため評価結果を踏まえた考察を行い、今後解決されるべき事項の整理を行った。

謝辞 本研究は JSPS 科研費 JP19K11972 の助成を受けたものです。

参考文献

[1] 伊豆 哲也他, “トコトンやさしい暗号の本”, 日刊工業新聞社, 2010
[2] Manuel Egele, David Brumley, Yanick Fratantonio, and Christopher Kruegel. 2013. An empirical study of cryptographic misuse in android applications. In Proc. of the 2013 ACM SIGSAC conference on Computer & communications security (CCS ’13)
[3] David Lazar, Haogang Chen, Xi Wang, and Nickolai Zeldovich. 2014. Why does cryptographic software fail?: a case study and open problems. In Proc. of 5th Asia-Pacific Workshop on Systems (APSys ’14)
[4] Li Y., Zhang Y., Li J., Gu D. (2014) iCryptoTracer: Dynamic Analysis on Misuse of Cryptography Functions in iOS Applications. In Network and System Security. NSS 2015
[5] Alexia Chatzikonstantinou, Christoforos Ntantogian, Georgios Karopoulos, and Christos Xenakis. 2016. Evaluation of Cryptography Usage in Android Applications. In Proc. of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS) (BICT’15)
[6] Y. Acar, S. Fahl and M. L. Mazurek, ”You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users,” 2016 IEEE Cybersecurity Development (SecDev)
[7] Y. Acar, M. Backes, S. Fahl, D. Kim, M. L. Mazurek and C. Stransky, ”You Get Where You’re Looking for: The Impact of Information Sources on Code Security,” 2016 IEEE Symposium on Security and Privacy (SP)
[8] Steven Arzt, Sarah Nadi, Karim Ali, Eric Bodden, Sebastian Erdweg, and Mira Mezini. 2015. Towards secure integration of cryptographic software. In 2015 ACM International Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software (Onward!) (Onward! 2015)
[9] Stefan Krüger, Sarah Nadi, Michael Reif, Karim Ali, Mira Mezini, Eric Bodden, Florian Göpfert, Felix Günther, Christian Weinert, Daniel Demmler, and Ram Kamath. 2017. CogniCrypt: supporting developers in using cryptography. In Proc. of the 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE 2017)
[10] Siqi Ma, David Lo, Teng Li, and Robert H. Deng. 2016. CDRep: Automatic Repair of Cryptographic Misuses in Android Applications. In Proc. of the 11th ACM on Asia Conference on Computer and Communications Security (ASIA CCS ’16)
[11] Duc Cuong Nguyen, Dominik Wermke, Yasemin Acar, Michael Backes, Charles Weir, and Sascha Fahl. 2017. A Stitch in Time: Supporting Android Developers in WritingSecure Code. In Proc. of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS ’17)
[12] Sideways Dictionary, `https://sidewaysdictionary.com/\#/`, （参照 2021-1-27）
[13] Art of the Problem.” Public key cryptography - Diffie-Hellman Key Exchange (full version)”.YouTube.2012-7-30. `https://www.youtube.com/watch?v=YEBfamv-_do`,(参照 2020-11-19)
[14] PILOT.”よくあるご質問”.PILOT ホームページ.2020-10-18. `https://www.pilot.co.jp/support/frixion/1334578774507.html`,(参照 2020-11-18)