Vol.2022-SPT-46 No.30
2022/3/8

等価的物理モデリングを用いた暗号技術のユーザ理解度評価

山下 雄大[1,a)]　金岡 晃[1,b)]

概要：暗号を専門としていない技術者に、わかりやすい表現や直感的な例を用いて暗号技術について理解を促すこと目的とした等価的物理モデルに対して、その有効性を測る。その実証として、RSA、Diffie-Hellman 鍵交換、楕円曲線 Diffie-Hellman 鍵交換を対象に検討した物理モデルについて、それらを使用して説明した場合と、そうでない場合で説明した際に、理解度にどれほどの差が発生するかの実験を行う。また、実験結果を Kruskal-Wallis 検定や Mann-Whiteny U 検定を用いて評価する。

1. はじめに

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する場合があることがこれまでの研究により明らかになっている。

暗号技術の誤使用を解決する手段として、暗号技術の理解が少なくても適切に暗号技術を使用できるように開発の場面において自動化や支援を行う技術の開発研究がある。また、別のアプローチとして暗号技術を適切に使用できるように技術者に理解を促す方法がある。本研究では後者のアプローチに焦点を当てる。

石島らの研究 [1] では、暗号を専門としていない技術者に分かりやすい表現や直感的な例を用いて暗号技術についての理解を促すことを目的として、暗号技術の等価的物理モデリングの実現方法の検討を行い、その手段として比喩を用いた解説に着目した。石島らの研究では、比喩による要素の置き換えのことをモデリングと呼び、置き換えられたものを物理モデルとした。技術用語を物理モデルにより表現する場合、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が非常に重要になることから、石島らの研究では「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」という 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した。

石島らの研究では、上記の定義をもとに RSA、Diffie-Hellman 鍵交換、楕円曲線 Diffie-Hellman 鍵交換を対象に等価的物理モデリングの検討と評価を行った。しかし、考察した物理モデルの効果に関する評価が不足していることが課題となっていた。

そこで本研究では、石島らが提案した物理モデルが効果的かどうかを評価するために、RSA、Diffie-Hellman 鍵交換、楕円曲線 Diffie-Hellman 鍵交換を対象に、物理モデルを用いて説明した場合と、そうでない場合で説明した際に、理解度にどれほどの差が発生するかのユーザ実験を行う。ユーザ実験にあたり、石島らが考案した物理モデルの再現を行い、その後物理モデルを用いた解説動画とそれ以外の表現モデルを用いた解説動画を作成する。実験では解説動画の視聴後に理解度調査と事後アンケートをとり、その結果から物理モデルの効果を分析する。

理解度調査結果と事後アンケートについて検定を行った結果、理解度の面からは表現モデルの差による学習効果は認められなかったが実験参加者の自己評価では効率的な理解ができたという反応を得た。

2. 関連研究

暗号技術の誤使用に関する研究は、広くなされている。Egele ら [2] や Lazer ら [3]、Chatzikonstantinou ら [4] は暗号 API の適切な利用の困難性を示し、いずれも暗号理論として基礎的な技術といえる共通鍵暗号の利用モードや RSA 暗号の利用で誤使用が発生していることを明らかにした。

誤使用への対策は、暗号技術の理解が少なくても適切に暗号技術を使用できるよな自動化や支援技術の研究と、暗号技術を適切に使用できるように技術者に理解を促す研究に大別できる。先述した石島らの研究は後者にあたる。

前者に当たるアプローチは、いくつかのアプローチで研究されている。まず、2015 年に Arzt らによって Eclipse

1 東邦大学
Toho Uniersity
a) 5518099y@st.toho-u.jp
b) akira.kanaoka@sci.toho-u.ac.jp

ⓒ 2022 Information Processing Society of Japan

のプラグインとして提案がされた [5]。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 [6]。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 [7]。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 [8]。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. 暗号技術の等価的物理モデリング

石島らの研究では、暗号を専門としていない技術者に、わかりやすい表現や直感的な例を用いて暗号技術について理解を促すことを目的として、暗号技術の等価的物理モデリングの実現方法の検討を行った。

3.1 等価的物理モデリング

石島らの研究では、「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んでいる。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。そこで石島らの研究では、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した。

- 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

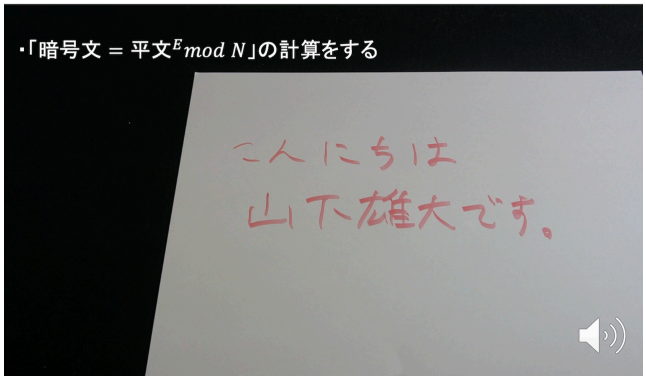

図 1　RSA の等価的物理モデルの利用例

3.2 等価的物理モデリングの評価基準

石島らは等価的物理モデリングの定義とともに、どのような物理モデルが等価的か判断するための基準も考察し、以下の 2 つに大別した。

- 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
- アルゴリズムごとの評価基準

3.3 物理モデルの評価と提案

石島らの研究では、RSA、DH を対象にした視覚的物理モデルと ECDH を対象にした味覚的物理モデルの検討を行った。

3.4 フリクションペンを用いた RSA の視覚的物理モデル

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を持つインキを用いたペンである。インク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。石島らの研究では消色させる手段としてアイロンを用いた。復色の手段として冷却スプレーを用いた。

RSA 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（図 1）。

3.4.1 評価基準に基づく評価

石島らは、評価基準に基づいて提案モデルの評価を行った。その結果を表 1 に示す。このモデルでは共通評価基準のみで評価を行った。

3.5 フリクションペンを用いた DH の視覚的物理モデル

RSA の視覚的物理モデルと同様にフリクションペンの特性を利用した。DH における G を紙、A と B を鍵交換

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	×

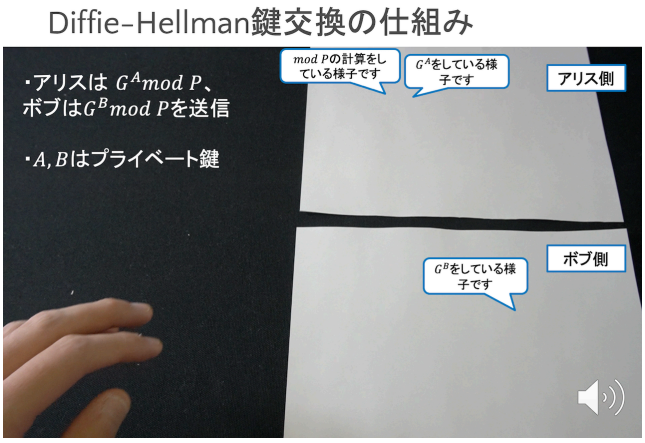

図 2　DH の等価的物理モデルの利用例

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	△

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	△

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（図 2）。

3.5.1　評価基準に基づく評価

石島らは評価基準に基づいて提案モデルの評価を行った。その結果を表 2 に示す。このモデルでは共通評価基準のみで評価を行った。

3.6　コーヒー、ミルク、ガムシロップを用いた ECDH の味覚的物理モデル

ECDH における G をコーヒーが入ったカップ、a をガムシロップの量、b をミルクの量とし、乗算をミルクまたはガムシロップをカップに入れ、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（図 3）。

3.6.1　評価基準に基づく評価

石島らは評価基準に基づいて提案モデルの評価を行った。その結果を表 3 に示す。このモデルでは共通評価基準のみで評価を行った。

図 3　ECDH の等価的物理モデルの利用例

4.　課題

石島らの研究では、暗号を専門としていない技術者に暗号技術について理解を促すことを目的として、等価的物理モデリングの実現方法を検討し、著者らが考案した物理モデルに対し評価を行なっている。しかし、石島らの研究では、考案した物理モデルが効果的かどうかの評価が不足している。具体的には、物理モデルを用いて暗号技術を説明した場合の理解度の評価である。そのため、RSA、DH、ECDH を対象に物理モデルを用いて説明した場合と、そうでない場合で説明した際に、理解度にどれほどの差が発生するかのユーザ実験を行い、物理モデルが効果的かどうか評価する必要がある。

5.　ユーザ実験の方法

石島らが提案したモデルに基づいて RSA、DH、ECDH の解説動画を作成し、理解度にどれほどの差が発生するかを測ることで等価的物理モデリングの効果を分析することを目的としたユーザ実験を行う。ここではユーザ実験に関わる要因や条件として、ユーザ実験のデータ収集方法やその分析方法について述べる。

5.1　暗号技術解説用動画の作成

石島らが提案した等価的物理モデルが効果的かどうか評価するためには、物理モデルの理解度を評価するだけではそのモデルの効果を測定することができないため、RSA、DH、ECDH に関して物理モデルを使用しない表現モデルを用いた場合の理解度も評価し、その差を比較する。

本実験では、理解度の評価のために暗号技術の解説を動画として作成し、その動画視聴により暗号技術の理解がどれだけされたかを測ることとした。

動画により暗号技術を解説するため、映像のほかに音声による解説が必要になる。動画を等価的物理モデルを用いたものと用いないものを用意した場合、両者の動画におい

表 4　RSA 解説動画の URL

RSA	
https://www.youtube.com/watch?v=-g1IIi12exI	音声のみ
https://www.youtube.com/watch?v=u0xqYdqywd0	図あり
https://www.youtube.com/watch?v=dq8M1QCZQng	物理モデル

表 5　DH 解説動画の URL

DH	
https://www.youtube.com/watch?v=VzMtPAbCoyU	音声のみ
https://www.youtube.com/watch?v=XOn3dt0y8iE	図あり
https://www.youtube.com/watch?v=y8B3LeUBIkg	物理モデル

て同様の解説を行わなければ、解説の差により理解度の度合いが変わってしまう可能性が考えられる。それにより、実験の結果で現れた差がモデルの差によるものなのか、解説の差によるものなのか判断がつかなくなってしまう。そのため、解説自体同じものを使用することとした。

1 つの暗号技術に対し複数の種類の解説動画を作るとき、解説自体を同じとするためまず動画のシナリオを作成した。シナリオでは動画の目的、視聴者の対象、動画の内容、解説するセリフを決める。

次に、シナリオに基づき絵コンテを作成し、動画の各シーンの内容を決める。そして作成したシナリオと絵コンテに基づき、解説資料の材料を準備する。最後に音声の収録や映像の撮影、資料の作成を行い、それらの材料より動画を作成する。

解説動画は、図表等は映像に現れず音声だけで解説をする「音声のみ」と、音声に加えて数式やブロック図と文字を映像で流す「図あり」と、「図あり」の映像に石島らが提案した等価的物理的モデリングを実際に準備して動作を撮影した動画を併せて表示した「物理モデル」の 3 種類を用意した。

5.2　ユーザ実験の手順

前節の方法で作成した RSA、DH、ECDH の解説動画を用いてユーザ実験を行う。実験は以下の手順で行う。

参加者の募集　Lancers で実験の参加者を募集する

実験の説明と意思確認　実験用サイトに移動し、実験の目的と内容の説明及び、実験に参加するか意思確認を行う

暗号技術の紹介　ランダムで RSA か DH か ECDH 用のページに移動する

動画の視聴　ランダムで物理モデルを用いた解説動画、音声のみの解説動画、図を用いた解説動画のいずれかを視聴する

理解度テストの実施　暗号技術に関しての、機能と安全性の根拠に関する理解度調査を実施する

アンケートの実施　実験に関するアンケートを実施する

報酬の支払い　実験の参加者に報酬を支払う

また、RSA、DH、ECDH それぞれの解説動画の URL を表 4、表 5、表 6 に示す。

5.3　理解度調査、アンケート調査の項目

理解度調査では、石島らが等価的物理モデリングの評価軸として設定したアルゴリズムの正確性や数学的な困難性の表現を測ることを考え、問 1 では公開鍵を用いたデータ送信をする際に利用すべき鍵の種類の選択、問 2 では各暗号技術における公開情報の選択、問 3 では各暗号技術の安全性の根拠となっている数学的な困難性、問 4 は各暗号技術の説明、についてそれぞれ 4 択から回答をしてもらった。

表 6　ECDH 解説動画の URL

ECDH	
https://www.youtube.com/watch?v=UgjTDlIA7Dk	音声のみ
https://www.youtube.com/watch?v=GfE44m77W6w	図あり
https://www.youtube.com/watch?v=TXeo413pDlc	物理モデル

設問	設問文
1	この動画は長い
2	この動画の解説はわかりやすかった
3	この動画により暗号技術の理解が深まった
4	この解説では細かいところまで理解ができない
5	動画による学習は書籍を読むよりも効果的
6	この動画を理解するために、他の知識を学ぶことが必要だ
7	この動画による学習は効果がある
8	この動画による学習は効率的である
9	この動画による学習に満足している

表 7　アンケート調査の設問

アンケート調査では、動画の長さ、解説のわかりやすさ、暗号技術の理解の有無と困難さ、解説による学習効果と効率、他の知識の必要性、満足などの項目を 9 つ用意し、5 段階の Likert 尺度より回答をしてもらった。設問を表 7 に示す。

5.4　ユーザ実験の実施

ユーザ実験は 2022 年 1 月 26 日にランサーズを通じて参加者を募集し実施された。報酬は 120 円を支払った。報酬金額は、あらかじめ著者らや著者が所属する組織の者によるユーザ実験シミュレーションから得られた実験に従事するための時間や、地域の最低賃金をもとに決定した。

900 人が実験に参加し、そのうち実験サーバ上の登録情報とランサーズ上の登録情報の照合に合致しなかったデータや、実験の回答に失敗しているデータを取り除いた 860 人分のデータに対して分析を行った。

参加した 900 人のうち、男性が 53.95%、女性が 46.05%であった。また最も多い年齢層は 30 歳代で 301 人 (35.00%)、次いで 40 歳代が 270 人 (31.40%) であった。利用された環境は、PC からの利用が 79.88%、スマートフォンが 16.51%、タブレットが 3.60%であった。

表 8　ユーザ実験において各動画に割り当てられた人数

暗号技術	音声のみ	図あり	物理モデル	小計
RSA	97	109	95	301
ECDH	93	93	91	277
DH	86	98	98	282

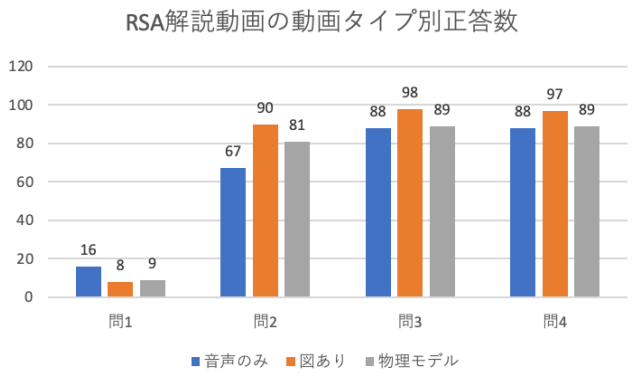

図 4　RSA 解説動画の動画タイプ別正答数

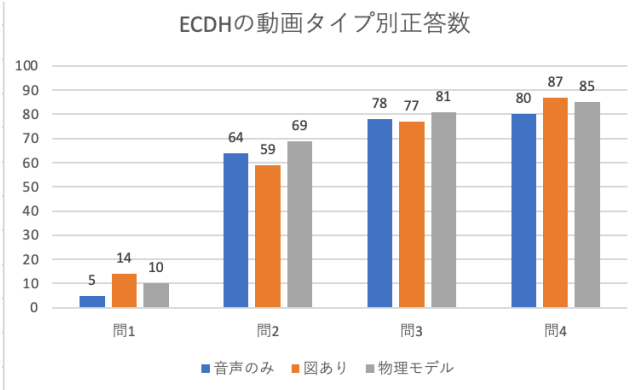

図 5　ECDH 解説動画の動画タイプ別正答数

それぞれの暗号技術や動画タイプに割り当てられた実験参加者数を表 8 に表す。

5.5　実験結果

RSA、DH、ECDH 解説動画における理解度調査の正答数をそれぞれ図 4、5、6 に示す。また、RSA、DH、ECDH 解説動画におけるアンケートの回答結果をそれぞれ図 7、8、9、10、11、12、13、14、15 にそれぞれ示す。

5.5.1　検定の実施

理解度調査の正答数及び、アンケートの回答結果について Kruskal-Wallis 検定と Mann-Whitney U 検定を用いて評価を行う。評価には統計ソフトの EZR を利用した。

まず Kruscal-Walli 検定により 3 群（音声のみ、図あり、物理モデル）の回答に有意差があるかを検定し、P 値が $P < 0.05$ ならば、「有意差あり」とし、それぞれの 2 群の間の検定を Mann-Whitney U 検定を実施した。

5.6　評価結果

理解度調査の検定を行ったところ、各暗号技術について

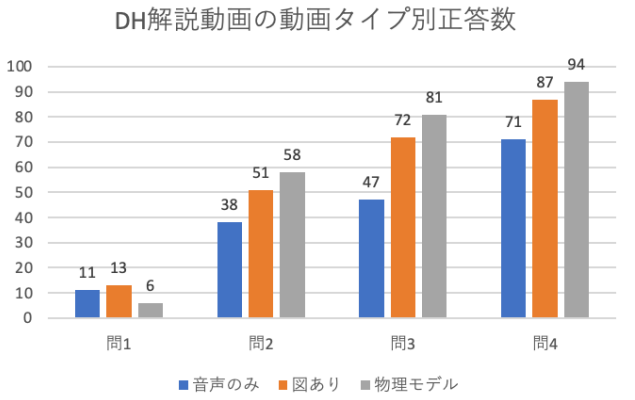

図 6　DH 解説動画の動画タイプ別正答数

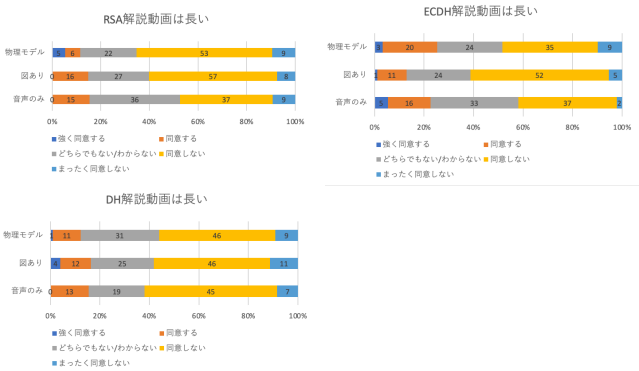

図 7　RSA、DH、ECDH 解説動画における設問 1 の回答

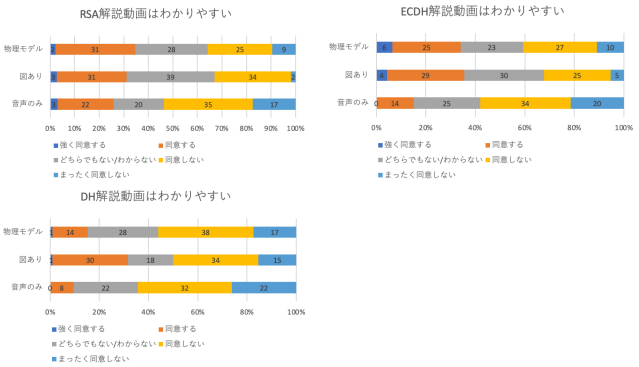

図 8　RSA、DH、ECDH 解説動画における設問 2 の回答

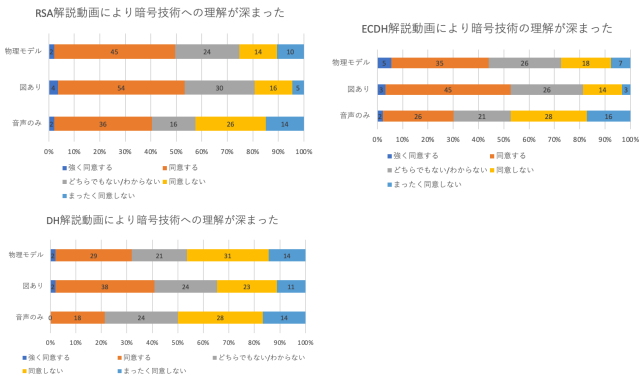

図 9　RSA、DH、ECDH 解説動画における設問 3 の回答

のいずれに結果についても Kruscal-Wallis 検定の結果は P 値が 0.05 を下回ることはなく、有意差なしと判定された。

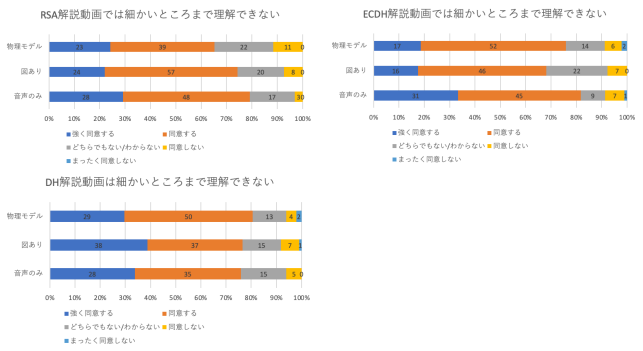

図 10　RSA、DH、ECDH 解説動画における設問 4 の回答

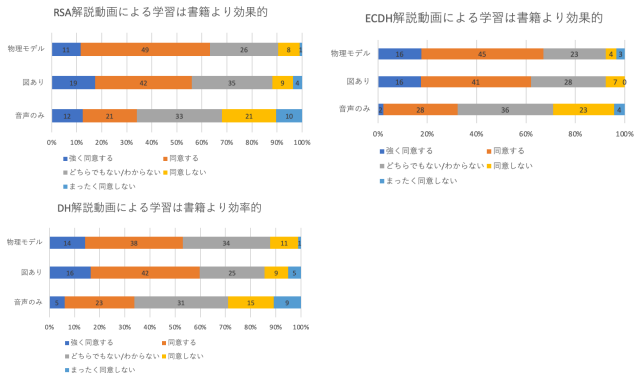

図 11　RSA、DH、ECDH 解説動画における設問 5 の回答

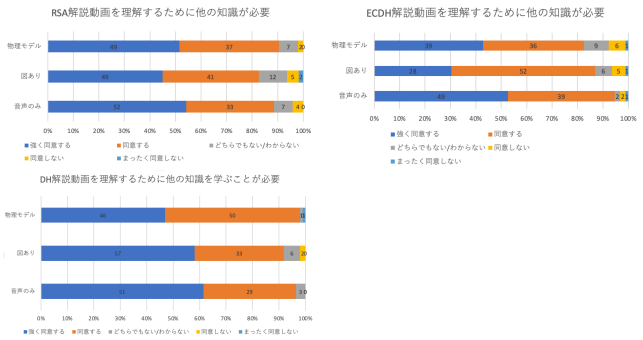

図 12　RSA、DH、ECDH 解説動画における設問 6 の回答

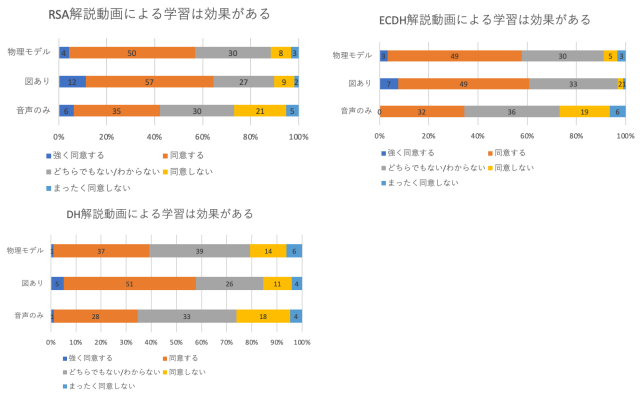

図 13　RSA、DH、ECDH 解説動画における設問 7 の回答

アンケート回答結果についての Kruscal-Wallis 検定の結果を表 9 に示す。いくつかの設問においては有意差なしと判定されたが、多くの設問が有意差ありと判定された。有意さありと判定されたものについて Mann-Whitney U 検

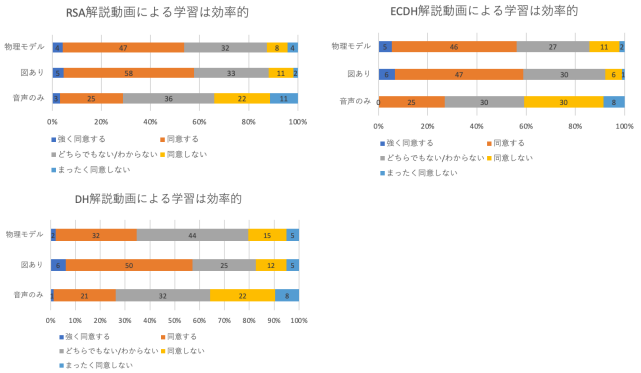

図 14　RSA、DH、ECDH 解説動画における設問 8 の回答

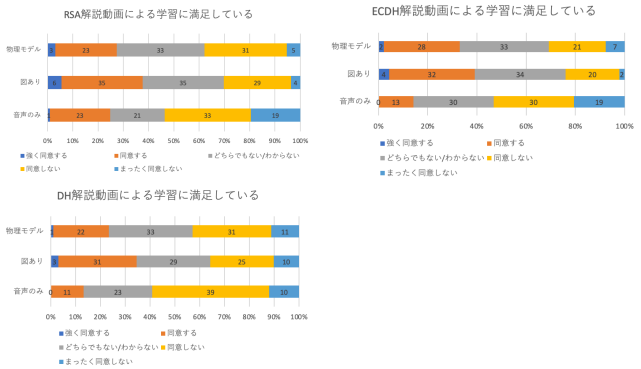

図 15　RSA、DH、ECDH 解説動画における設問 9 の回答

定を実施した結果を、それぞれ暗号ごとに表 10、11、12 に示す。RSA、ECDH、DH の解説動画について、音声のみの解説動画を 1(以後動画タイプ 1 とする)、図を用いた解説動画を 2(以後動画タイプ 2 とする)、物理モデルを用いた解説動画を 3(以後動画タイプ 3 とする) として検定を行った。

Mann-Whitney U 検定を行った結果、RSA 解説動画では、設問 2、設問 5、設問 7、設問 8、設問 9 において、動画タイプ 1 と 2 及び、1 と 3 の間で「有意差あり」となった。設問 3 は、1 と 2 の間のみ「有意差あり」となった。ECDH 解説動画では、設問 2、設問 3、設問 5、設問 6、設問 7、設問 8、設問 9 において、動画タイプ 1 と 2 及び、1 と 3 の間で「有意差あり」となった。DH 解説動画では、設問 5、設問 7、設問 8、設問 9 において、動画タイプ 1 と 2 及び、1 と 3 の間で「有意差あり」となった。設問 2、設問 3 では、1 と 2 の間のみ「有意差あり」となった。

6.　考察

RSA、ECDH、DH 解説動画におけるアンケートの回答結果について、設問 1「この動画は長い」に関しては、それぞれの解説動画の間に有意差は見られなかったため、それぞれの解説動画の動画タイプにおいて、特定の動画タイプのみ長いと感じることはないと言えるだろう。

設問 2「この動画の解説はわかりやすかった」に関しては、RSA、ECDH、DH の全ての場合で有意差が出ていた。

設問	RSA	ECDH	DH
1	0.156	0.026	0.939
2	0.114	0.000	0.012
3	0.017	0.000	0.028
4	0.138	0.022	0.831
5	0.000	0.000	0.000
6	0.243	0.007	0.208
7	0.001	0.000	0.004
8	0.000	0.000	0.000
9	0.000	0.000	0.003

表 9 RSA、ECDH、DH 解説動画のアンケート回答結果について Kruskal-Wallis 検定を行った結果の P 値

設問	1,2	1,3	2,3
2	0.004	0.003	0.768
3	0.004	0.081	0.328
5	0.000	0.000	0.684
7	0.000	0.026	0.136
8	0.000	0.000	0.569
9	0.000	0.024	0.110

表 10 RSA 解説動画におけるアンケート結果について Mann-Whiteny U 検定を行った結果

設問	1,2	1,3	2,3
2	0.000	0.002	0.404
3	0.000	0.005	0.199
5	0.000	0.000	0.649
6	0.001	0.055	0.321
7	0.000	0.000	0.325
8	0.000	0.000	0.460
9	0.000	0.000	0.193

表 11 ECDH 解説動画におけるアンケート結果について Mann-Whiteny U 検定を行った結果

設問	1,2	1,3	2,3
2	0.004	0.111	0.123
3	0.007	0.277	0.122
5	0.000	0.001	0.559
7	0.002	0.436	0.012
8	0.000	0.037	0.008
9	0.001	0.040	0.135

表 12 DH 解説動画におけるアンケート結果について Mann-Whiteny U 検定を行った結果

特に、RSA、ECDH では、動画タイプ 1、2 と 1、3 の間に、DH では動画タイプ 1、2 の間に有意差が出ていたことから、RSA、ECDH、DH 解説動画のいずれにおいて、音声のみの解説はわかりにくいことが言えるだろう。

設問 3「この動画により暗号技術の理解が深まった」では、RSA、ECDH、DH の全ての場合で有意差が出ていた。特に RSA、DH では、動画タイプ 1、2 の間に、ECDH では動画タイプ 1、2 と 1、3 の間に有意差が出ていたことから、RSA、ECDH、DH 解説動画のいずれにおいて、音声のみの解説では理解が深まらないことが言えるだろう。

設問 4「この解説では細かいところまで理解ができない」では、RSA、ECDH、DH の間に有意差は見られなかったため、それぞれの動画のいずれの動画タイプにおいて、理解できないと感じていることが言えるだろう。

設問 5「動画による学習は書籍を読むよりも効果的だ」では、RSA、ECDH、DH の全ての場合で有意差が出ていた。また、それぞれの暗号技術解説動画の動画タイプ 1、2 と 1、3 の間で有意差が出ていたことから、RSA、ECDH、DH 解説動画のいずれにおいて、音声のみの解説では書籍を読むよりも効果的ではないことが言えるだろう。

設問 6「この動画を理解するために、他の知識を学ぶことが必要だ」では、ECDH のみ有意差が出た。特に動画タイプ 1、2 の間に有意差が出ていた。アンケート結果の分布を見てみると、「同意する」の量に差が出ているため、図を用いた解説動画の方が、音声のみの解説動画より他の知識を不要と思わせていたことがわかる。全体で見ると「同意する」が多いため、RSA、ECDH、DH 解説動画を理解するためには他の知識を学ぶ必要があると感じていることが言えるだろう。

設問 7「この動画による学習は効果がある」では、RSA、ECDH、DH の全ての場合で有意差が出ていた。特に、RSA、ECDH では、動画タイプ 1、2 と 1、3 の間に、DH では 1、2 と 2、3 の間に有意差が出ていたため、RSA、ECDH 解説動画においては、音声のみの解説では学習に効果がないと感じていることが言えるだろう。また、DH 解説動画においては、図を用いた解説動画において「同意する」の量が多いことから、他の 2 つの動画タイプより効果があると感じていることが言えるだろう。

設問 8「この動画による学習は効率的である」では、RSA、ECDH、DH の全ての場合で有意差が出ていた。また、それぞれの暗号技術解説動画の動画タイプ 1、2 と 1、3 の間で有意差が出ていたことから、RSA、ECDH、DH 解説動画のいずれにおいて、音声のみの解説での学習は効率的とは言えないだろう。

設問 9「この動画による学習に満足している」では、RSA、ECDH、DH の全ての場合で有意差が出ていた。また、それぞれの暗号技術解説動画の動画タイプ 1、2 と 1、3 の間で有意差が出ていたことから、RSA、ECDH、DH 解説動画のいずれにおいて、音声のみの解説での学習は満足していないことが言えるだろう。

理解度調査の正答数については、RSA、ECDH、DH の全ての場合で有意差は見られなかった。また、理解度調査の回答についても、RSA において問 1、問 2 のみ動画タイプ 1、2 と 1、3 の間で有意差が見られたが、動画コンテンツの違いで理解度向上に大きな差が出たとは言い難い結果となった。

上記の結果から言えることは、動画の差による学習効果

は認められないが、利用者としては図や物理モデルがあると満足度が高まり、効率的であり、分かりやすいという認識がある。このことから、音声のみで解説を行うよりも、図や物理モデルなどを用いて解説する方が効率的な学習ができたと感じていることがわかる。しかし、図と物理モデルの間に大きな差は見られなかった。

いずれの動画タイプにおいても「他の知識が必要」、「細かいところまでの理解ができていない」という結果が出ている。この結果の原因は、いくつか考えられ 1 つに限定することは今回の結果からは難しい。考えうる原因を以下に挙げる。

- 物理モデリングというアプローチの意味が少ない／ない
- 物理モデリングにおける対象とするモデルの意味が少ない／ない
- 作成したシナリオが効果的でない
- 撮影した動画が効果的でない
- 作成した動画が効果的でない

上記のいずれも本ユーザ実験では明確に分析できる内容になっていなかったため、上記の内容を分析することが今後の課題となる。

7. まとめ

本研究では、石島らが考案した物理モデルに対して、物理モデルが効果的かどうか評価するために RSA、DH、ECDH を対象に物理モデルを用いて説明した場合と、その他の表現モデルを用いて説明した場合で理解度にどれほどの差が発生するのかのユーザ実験を行った。実験に先立ち、石島らが考案した物理モデルの再現を行った。また、実験用の比較動画作成のテストとしてスキュタレー暗号を用いて、比較動画作成手順の詳細内容の洗い出しを行った。そして、それをもとに RSA、DH、ECDH を音声のみで解説した動画、図を用いて解説した動画および、物理モデルを用いて解説した動画を作成した。作成した動画を用いてユーザ実験を行い、結果を評価した。評価の結果、図や物理モデルを用いて解説する方が、音声のみで解説するよりも効率的な学習ができたと感じていることがわかった。しかし、表現モデルの差による学習効果は認められなかった。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課題の整理を行った。

謝辞　本研究の一部は JSPS 科研費 JP19K11972 の助成を受けたものです。

参考文献

[1] 石島慧, 金岡晃. ”暗号技術の等価的な物理的モデル化検討.” 研究報告セキュリティ心理学とトラスト (SPT) 2021.15 (2021): 1-8.

[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] 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)

[5] 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)

[6] 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)

[7] 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)

[8] 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)

ⓒ 2022 Information Processing Society of Japan