情報セキュリティアンプラグド ～計算機を用いない情報セキュリティ教育～

駒野 雄一[1]　水木 敬明[2]

概要：カードベースプロトコルやコインベースプロトコルは、身近に存在するカード（トランプ）やコイン（硬貨）を用いて人手でマルチパーティ計算を実現する技術である。本稿は、これらの物理的暗号技術に対して、故意や過失による異常操作が確率的に生じるモデルの下で、プロトコルから漏洩する情報を体系的に評価する手法を提案する。そして、提案手法を既存のプロトコルに適用し、その効果を確認する。さらに、“情報セキュリティは難しい” という先入観からなる学習障壁の低減と、情報セキュリティ的思考の養成の観点から、情報セキュリティ教育への物理的暗号技術の応用可能性を論じる。

キーワード：カードベースプロトコル, コインベースプロトコル, コンピュータサイエンス・アンプラグド

Information Security Unplugged: Education on Information Security without a Computer

Yuichi Komano[1]　Takaaki Mizuki[2]

Abstract: Card-based and coin-based protocols execute secure multi-party computations using a deck of physical playing cards and a set of coins, respectively. These protocols are useful not only for solving a social problem safely without any black-box computer but also for educating students about the principle of secure cryptographic protocols. In this paper, we first research information leakage from (un)intended operative errors and countermeasures against the errors. We then discuss the possibility of applying these protocols including the errors and countermeasures to education on the information security.

Keywords: card-based protocol, coin-based protocol, computer science unplugged

1. はじめに

マルチパーティ計算は、複数のユーザが互いの入力を秘匿したまま所望の値を計算するための技術であり、企業間のマーケティング情報の集計などへの応用が議論されている。一方、計算機を利用せずにマルチパーティ計算を実現する技術として、**カードベースプロトコル** [1] や**コインベースプロトコル** [6] が提案されている。これらの物理的暗号技術は、計算機をブラックボックス利用しないためにユーザが安心してプロトコルを実行できることに加えて、プロトコルの原理を直感的に理解しやすいために情報セキュリティ教育にも有用である。

物理的暗号技術は簡単に実装（実行）できる処理で構成されるが、ユーザは操作の向きや手順などを誤ってしまうことがある。文献 [5] は、プロトコルの各ステップにおいて、秘匿すべき入力の漏洩情報量を評価するための指標として**確率トレース**の概念を提案し、Koch らのダイアグラム [2] を拡張した**拡張ダイアグラム**を提案した。そして、6 枚のカードを用いる AND プロトコル [4] を例として、ユーザがカード巡回の向きを誤った場合に入力の情報が漏れる場合があることを示し、情報漏洩への対策を提案した。

情報セキュリティの教育においては、プロトコルを正しく実行した場合に所望の値を正しく計算できるという**完全**

[1] 東芝 研究開発センター
Corporate R&D Center, Toshiba Corporation
[2] 東北大学 サイバーサイエンスセンター
Cyberscience Center, Tohoku University

性を理解させることに加えて、故意や過失により異常な処理が発生した際に生じうる被害を把握して対策を考案する（**リスク分析と対策立案**）など情報セキュリティの考え方を理解させる必要がある。本稿は、物理的暗号技術における異常処理からの情報漏洩の議論を深めるとともに、情報セキュリティ教育への有用性を議論する。

本稿の貢献は以下のとおり。

(1) プロトコルの誤操作による情報漏洩の議論を進展する。まず、カードベースプロトコルに対して、文献 [5] の議論を拡張して、体系的に情報漏洩を評価する手法を与える。さらに、コインベースプロトコルに対して、誤操作による情報漏洩を議論する。

(2) 次に、物理的暗号技術と誤操作を含むプロトコルの評価が、情報セキュリティ教育に有用であることを議論する。これらの技術や評価に基づき、カードやコインを用いて情報セキュリティの考え方を直感的に学ぶことができるために "**情報セキュリティは難しいという先入観**" を取り除くことができると期待できる。そのため、情報セキュリティの初学者だけでなく、社会人へのリカレント教育にも有用である。本稿では、計算機を用いずに計算機科学教育を行う *Computer Science Unplugged* (CS-Unplugged, [9]) をなぞらえて、これらを**情報セキュリティアンプラグド** (Information Security Unplugged) とよぶことにする。

2. 物理的暗号技術

本節では、物理的暗号技術の既存研究として、カードベースプロトコルとコインベースプロトコルを復習する。

2.1 カードベースプロトコル

カードベースプロトコルは、表面に $\boxed{\clubsuit}$ や $\boxed{\heartsuit}$ の模様が描かれており、裏面がともに $\boxed{?}$ となるカードを使用して、マルチパーティ計算を実行する。ユーザは、自身の入力を

$$\boxed{\clubsuit}\boxed{\heartsuit} = 0, \quad \boxed{\heartsuit}\boxed{\clubsuit} = 1 \tag{1}$$

のようにエンコードして、カードをテーブルに裏返して並べ、所定の規則で操作する。例えば、6 枚のカードを用いる AND プロトコル $\mathcal{P}^{\mathsf{MS}}$ [4] は、以下の手順で実行される。

---

6 枚カード AND プロトコル $\mathcal{P}^{\mathsf{MS}}$
入力集合:

$$\left\{\Gamma_0^{00} = \left(\frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}\right), \Gamma_0^{01} = \left(\frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}\right),\right.$$
$$\left.\Gamma_0^{10} = \left(\frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}\right), \Gamma_0^{11} = \left(\frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}\right)\right\}$$

ステップ:

(1) $(\mathsf{turn}, \{3,4\})$

(2) $(\mathsf{perm}, (2\,4\,3))$

(3) $(\mathsf{shuf}, \{\mathsf{id}, (1\,4)(2\,5)(3\,6)\})$

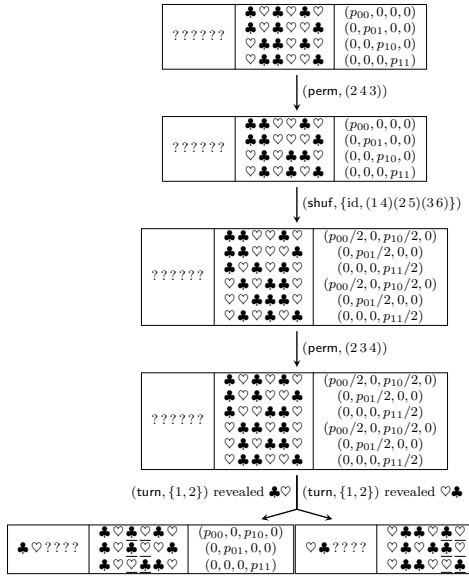

図 1 6 枚カード AND プロトコル $\mathcal{P}^{\mathsf{MS}}$ の状態遷移

(4) $(\mathsf{perm}, (2\,3\,4))$

(5) $(\mathsf{turn}, \{1,2\})$
if visible seq. $= (\clubsuit, \heartsuit, ?, ?, ?, ?)$ **then** $(\mathsf{result}, 3, 4)$
else if visible seq. $= (\heartsuit, \clubsuit, ?, ?, ?, ?)$ **then** $(\mathsf{result}, 5, 6)$

ここで、Γ_0^{ab} は、二人のユーザのそれぞれの入力 $a, b \in \{0,1\}$ に対応した、カードの初期配置をあらわす。例えば、Γ_0^{01} は、次のように設定される。Alice は、(1) 式に従って、入力 $a = 0$ に対応する $\boxed{\clubsuit}, \boxed{\heartsuit}$ を裏返してテーブルの左側に並べる。同様に、Bob は、入力 $a = 1$ に対応する $\boxed{\heartsuit}, \boxed{\clubsuit}$ を裏返してテーブルの右側に並べる。それらのカードの間には、$\boxed{\clubsuit}, \boxed{\heartsuit}$ を表向きに並べる。

上の実行例において、turn などはカードに対する操作をあらわす。(turn, T) は、T に含まれる番号のカードを裏返す操作である。(perm, σ) は、カード列に対して、置換 σ を施す。ステップ 2（および 4）では、2 から 4 枚目の 3 枚のカードに対して、左巡回シフト（および右巡回シフト）を施す。$(\mathsf{shuf}, \{\sigma_1, \sigma_2\})$ は、カード列に対して、置換 σ_1 か σ_2 をランダムに選択して施す。ステップ (3) では、6 枚のカード列を 3 枚ずつに分割し、それぞれの 3 枚の順番は維持したまま分割したカードをランダムに入れ替える。ステップ (5) は、裏返した左側 2 枚のカードが $\boxed{\clubsuit}, \boxed{\heartsuit}$（あるいは $\boxed{\heartsuit}, \boxed{\clubsuit}$）である場合には、3 枚目と 4 枚目（あるいは 5 枚目と 6 枚目）のカードに AND の結果が格納されていることをあらわす。詳細は [3], [4] を参照されたい。

図 1 は、$\mathcal{P}^{\mathsf{MS}}$ への拡張ダイアグラム [5] の適用例である。各ノードは、それぞれのステップでの、ユーザが目にするカード列（**可視化列**とよぶ）、すべて表面にした場合のカード列（**原始列**とよぶ）、確率トレースからなる。確率トレースは、すべての入力の組合せに対応した条件付確率からな

る組である。入力に対応する各成分は、可視化列を条件として、原始列と入力の同時確率をあらわす。図 1 の最終ステップにおいて、AND の結果は下線で示したカードに正しく格納されていること（**完全性**）を確認できる。また、最終ステップの左右の各ノードにおいて、確率トレースの和は入力時点での和 $(p_{00}, p_{01}, p_{10}, p_{11})$ と等しいことから、入力と可視化列は独立であり情報を漏らさないこと（**安全性**）を確認できる。詳細は [5] を参照されたい。

2.2 コインベースプロトコル

コインベースプロトコルは、カードの代わりにコインを利用するマルチパーティ計算技術である。裏返せば情報を秘匿できるカードと異なり、コインを積み重ねたり手で覆ったりして、情報を秘匿しながら計算を実行する。コインの表と裏を $\circ$ と $\bullet$ であらわす。ユーザは、自身の入力を

$$\bullet = 0, \quad \circ = 1 \tag{2}$$

のようにエンコードして、コインを掌中やテーブルに配置し、所定の規則で操作する。例えば、6 枚のコインを用いる AND プロトコル $\mathcal{P}^{\mathsf{AND}}_{\mathsf{Coin}}$ [6] は、以下の手順で実行される。

---

6 枚コイン AND プロトコル $\mathcal{P}^{\mathsf{AND}}_{\mathsf{Coin}}$

入力集合:

$$\Big\{\Gamma^{00}_0 = (\circ, \circ|\circ\bullet, \bullet\bullet|\epsilon, \epsilon, \epsilon, \epsilon), \Gamma^{01}_0 = (\circ, \circ|\bullet\bullet, \circ\bullet|\epsilon, \epsilon, \epsilon, \epsilon),$$
$$\Gamma^{10}_0 = (\bullet, \circ|\circ\bullet, \bullet\bullet|\epsilon, \epsilon, \epsilon, \epsilon), \Gamma^{11}_0 = (\bullet, \circ|\bullet\bullet, \circ\bullet|\epsilon, \epsilon, \epsilon, \epsilon)\Big\}$$

ステップ:

(1) $(\mathsf{hand}, \mathbf{A}_L \leftarrow \mathbf{B}_L)$
(2) $(\mathsf{hand}, \mathbf{A}_R \leftarrow \mathbf{B}_R)$
(3) $(\mathsf{move}, \mathbf{A}_L \rightarrow \mathbf{T}_1, 3)$
(4) $(\mathsf{move}, \mathbf{A}_R \rightarrow \mathbf{T}_2, 3)$
(5) $(\mathsf{shuffle}, \mathbf{T}_1, \mathbf{T}_2)$
(6) $(\mathsf{move}, \mathbf{T}_1 \rightarrow \mathbf{T}_3, 1)$
(7) $(\mathsf{move}, \mathbf{T}_2 \rightarrow \mathbf{T}_4, 1)$
(8) **if** $(\mathsf{top}(\mathbf{t}_1), \mathsf{top}(\mathbf{t}_2)) = (\circ, \bullet)$
$(\mathsf{result}, \mathsf{bottom}(\mathbf{t}_1))$
(9) **else if** $(\mathsf{top}(\mathbf{t}_1), \mathsf{top}(\mathbf{t}_2)) = (\bullet, \circ)$
$(\mathsf{result}, \mathsf{bottom}(\mathbf{t}_2))$

コインベースプロトコルでは、各ユーザの掌中とテーブルにコインを配置して処理を実行する。例えば、$\mathcal{P}^{\mathsf{AND}}_{\mathsf{Coin}}$ の入力 Γ^{10}_0 に対しては、次のようにコインが配置される。Alice は、(2) 式に従って、$\bar{a} = 0$ に対応するコイン $\bullet$ を左手 $\mathbf{A}_L$ に隠し持ち、右手 $\mathbf{A}_R$ にはコイン $\circ$ を持つ。Bob は、$b = 0$ に対して、左手 $\mathbf{B}_L$ にコイン $\bar{b}\bullet = \circ\bullet$ を隠し持ち、右手 $\mathbf{B}_R$ に $b\bullet = \bullet\bullet$ を隠し持つ。上述のプロトコルではテーブル $\mathbf{T}$ を 4 つの領域に分けて使用するが、入力の段階ではコインを配置しない。

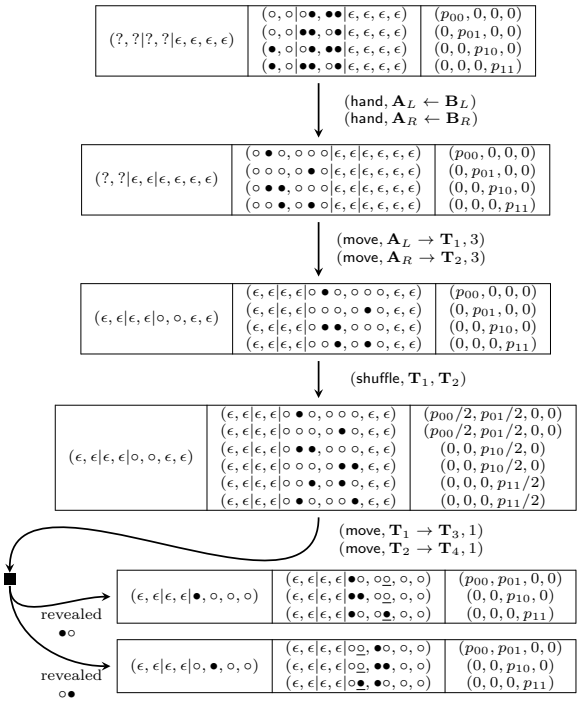

図 2 6 枚コイン AND プロトコル $\mathcal{P}^{\mathsf{AND}}_{\mathsf{Coin}}$ の状態遷移

上の実行例において、$(\mathsf{hand}, \mathbf{P}_1 \leftarrow \mathbf{P}_2)$ は、$\mathbf{P}_2$ の掌中にあるコインを $\mathbf{P}_1$ の掌中に移す操作をあらわす。具体的には、$\mathbf{P}_2$ を握ったまま $\mathbf{P}_1$ の上に重ねて、両方の手を同時に開き、コインが見えないように $\mathbf{P}_1$ を閉じる。$\mathbf{P}_1$ と $\mathbf{P}_2$ にコインを隠し持っていた場合には、$\mathbf{P}_1$ のコインの上に $\mathbf{P}_2$ のコインが反転して積み重なる。$(\mathsf{move}, \mathbf{P}_1 \rightarrow \mathbf{P}_2, n)$ は、$\mathbf{P}_1$ に配置されたコインの上から n 枚をつまみ上げて、$\mathbf{P}_2$ のコインの上に移す。$(\mathsf{shuffle}, \mathbf{P}_1, \mathbf{P}_2)$ は、$\mathbf{P}_1$ と $\mathbf{P}_2$ に置かれたコインをランダムに入れ替える。ステップ (8) および (9) は、テーブルの第 1 と第 2 の領域のコインが $\circ, \bullet$（あるいは $\bullet, \circ$）であるならば、第 1（あるいは第 2）の領域のコインのテーブル面に AND 結果が格納されていることをあらわす。詳細は [6] を参照されたい。

図 2 は、$\mathcal{P}^{\mathsf{AND}}_{\mathsf{Coin}}$ への拡張ダイアグラム [5] の適用例である。図 1 と同様に、$\mathcal{P}^{\mathsf{AND}}_{\mathsf{Coin}}$ の完全性と安全性を確認できる。

3. 誤操作を含むプロトコルからの情報漏洩

ユーザが物理的暗号技術の操作を誤ると、秘密すべき入力の情報が漏洩することを確認する。

3.1 誤操作を含む 6 枚カード AND プロトコル

文献 [5] は、2.1 節で紹介した $\mathcal{P}^{\mathsf{MS}}$ のステップ (2) と (4) において、ユーザが巡回シフトの向き（二つのステップの操作の向きを並べて「左右」のように記す）を間違えることで得られる 3 つのプロトコルを $\mathcal{P}_1$（右左）、$\mathcal{P}_2$（右右）、$\mathcal{P}_3$（左左）とおき、拡張ダイアグラムを利用して各プロト

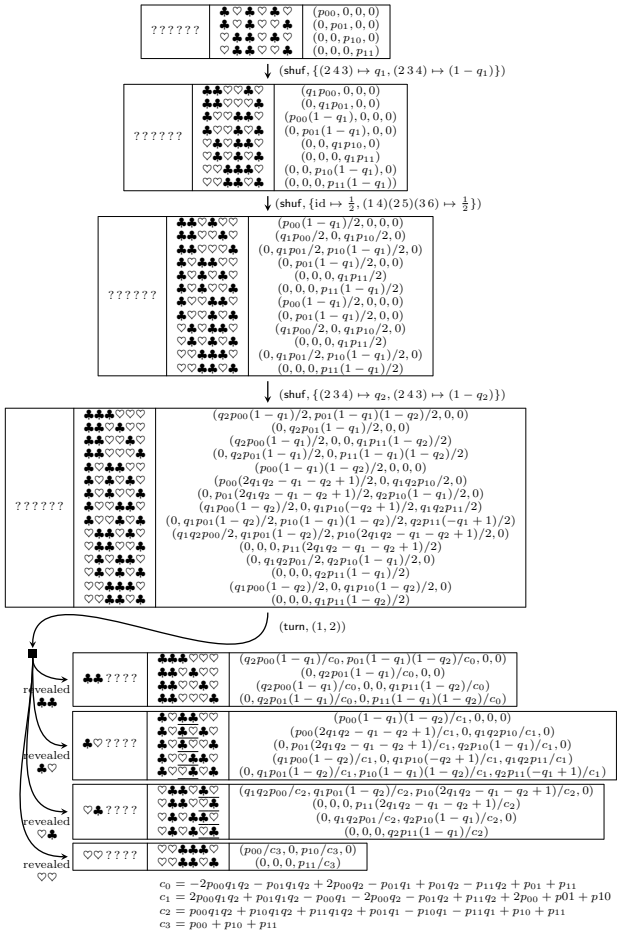

図 3　シフトの正誤を考慮した $\mathcal{P}^{\mathsf{MS}}$ の拡張ダイアグラム

コルの完全性と安全性を個別に議論した。

本稿は、各巡回シフトの正誤に関する確率変数を導入し、$\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ を体系的に評価する手法を提案する。

ステップ (2) と (4) で正しい向きに巡回シフトする確率を q_1, q_2 とおく。図 3 は、巡回シフトの正誤の確率を考慮した $\mathcal{P}^{\mathsf{MS}}$ への拡張ダイアグラムの適用結果である。図に示したように、巡回シフトの誤りは、シャッフルを用いて表現することができる。例えば、ステップ (2) の巡回シフトに相当する $(\mathsf{shuf}, \{(2\,4\,3) \mapsto q_1, (2\,3\,4) \mapsto (1-q_1)\})$ は、確率 q_1 で置換 $(2\,4\,3)$（正しい左巡回シフト）を実行し、確率 $(1-q_1)$ で置換 $(2\,3\,4)$（誤った右巡回シフト）を実行することをあらわす。 $q_1 = q_2 = 1$ のときには、$\mathcal{P}^{\mathsf{MS}}$ が正しく実行され、拡張ダイアグラムは図 1 と一致する。$q_1 = q_2 = 0$ のとき、[5] における $\mathcal{P}_1$ の評価に一致し、$(q_1, q_2) = (0, 1)$ と $(1, 0)$ が $\mathcal{P}_2$ と $\mathcal{P}_3$ の評価に一致することを確認できる。

図 3 の最終状態において、左側 2 枚のカードが ♣♣ あるいは ♡♡ となる場合には、$\mathcal{P}^{\mathsf{MS}}$ は異常終了する。例えば、♣♣ の場合には、確率トレースの和の第三成分が 0 となることから、入力が $(1, 0)$ 以外であることが分かる。あるいは、♡♡ の場合には、確率トレースの和は $(p_{00}/c_3, 0, p_{10}/c_3, p_{11}/c_3)$ であり、入力が $(0, 1)$ 以外であったことと、残る 3 通りの入力の比が $p_{00} : p_{10} : p_{11}$ であることが分かる。

また、左側 2 枚のカードが ♣♡ や ♡♣ の場合でも、出力（下線部）が不定な値や誤った値になる場合があることを確認できる。例えば、左側 2 枚のカードが ♣♡ である場合に、出力が (1) 式でデコードできない不定な ♣♣ となることがあり、このとき入力が $(0, 0)$ である条件付確率は $p_{00}(1-q_1)(1-q_2)/c_1$ である（ステップ (2) と (4) の両方で巡回シフトの向きを誤る、すなわち、$q_1 < 1$ かつ $q_2 < 1$ のときに生じる）ことを確認できる。同様に、♣♡ の 4 行目に示すように、入力が $(0, 0)$ であるにもかかわらず、誤った値 ♡♣ $= 1$ を確率 $q_1 p_{00}(1-q_2)/c_1$ で（ステップ (2) は正いが (4) は巡回シフトの向きを誤る、すなわち $q_1 = 1$ かつ $q_2 < 1$ のときに）出力することを確認できる。

文献 [5] は、$\mathcal{P}^{\mathsf{MS}}$ における誤操作を検出するために、左側 2 枚のカードを上下逆さまにしてプロトコルを実行する[*1]、などの手法を提案している。これらの手法は、本稿のように誤操作を確率的に記述した場合にも有効である。手法の詳細は [5] を参照されたい。

3.2　誤操作を含む 6 枚コイン AND プロトコル

文献 [6] は、コインを用いて、NOT, AND, OR, XOR, コピーを実行するプロトコルを提案し、それぞれの完全性と安全性を議論した。本稿は、コインベースプロトコルに対しても誤操作の概念を導入し、カードベースプロトコルと同様に、誤操作による情報漏洩を議論する。

2.2 節で紹介した 6 枚コイン AND プロトコル $\mathcal{P}^{\mathsf{AND}}_{\mathsf{Coin}}$ を考えよう。$\mathcal{P}^{\mathsf{AND}}_{\mathsf{Coin}}$ の処理は、コインを初期配置する、コインを手渡して束ねる、コインの束をテーブルに移す、コインの束をランダムに入れ換える、束の最上面のコインを取り除き AND 結果を得る、に分類される。このうち、コインを手渡して束ねる際に、対面で処理を実行すると、手の左右を取り間違える可能性がある。一方、その他の処理については、誤りが生じる可能性は低い。そこで、確率 $(1-q_1)$ で、ステップ (1) と (2) を以下の (1') と (2') に取り違える場合のプロトコルを考察する。

(1') $(\mathsf{hand}, \mathbf{A}_L \leftarrow \mathbf{B}_R)$

(2') $(\mathsf{hand}, \mathbf{A}_R \leftarrow \mathbf{B}_L)$

図 4 は、コインを渡す手の正誤の確率を考慮した $\mathcal{P}^{\mathsf{AND}}_{\mathsf{Coin}}$ への拡張ダイアグラムの適用結果である。$\mathcal{P}^{\mathsf{AND}}_{\mathsf{Coin}}$ でコインを渡す手を間違えると、$a \wedge b$ の代わりに $a \wedge \bar{b}$ が計算される。そのため、図 3 で見たような、処理が不定となる（左側 2 枚のカードが ♣♣ となる）事象や、AND 結果が不定となる（演算結果に対応するカードが ♣♣ となる）事象は生じない。

また、図 4 の各ノードにおける確率トレースの和は

[*1] $\mathcal{P}^{\mathsf{MS}}$ を正しく実行するとステップ (5) の左側 2 枚のカードの上下が逆さまになり、巡回シフトの向きを誤ると（一部の場合を除いて）異なるカードが上下逆さまになる。従って、ステップ (5) におけるカードの上下の向きに着目すれば、巡回シフトの誤操作を検出できる。

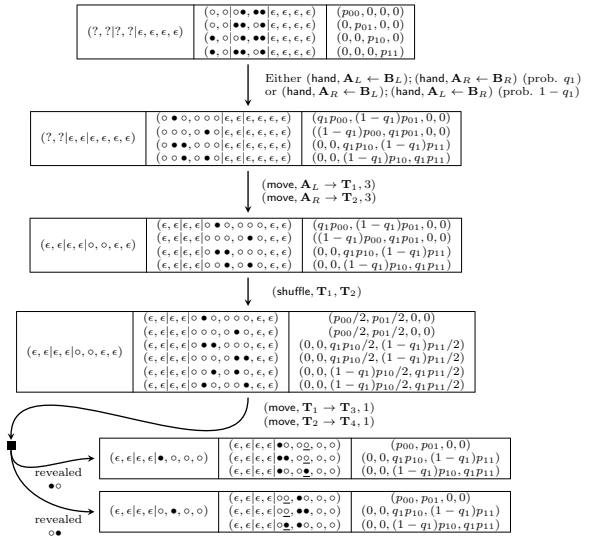

図 4 hand の正誤を考慮した $\mathcal{P}^{\mathsf{AND}}_{\mathsf{Coin}}$ の拡張ダイアグラム

$(p_{00}, p_{01}, p_{10}, p_{11})$ であり、コインを渡す手を確率的に誤る場合においては情報漏洩が起こらないことも確認できる。

一方、上述したとおり、誤操作により $a \wedge b$ ではなく $a \wedge \bar{b}$ が計算される。そのため、図 4 の一番下のノードの 2 行目のように、確率 $(1-q_1)p_{11}$ で、$(1,1)$ を入力しても演算結果が 0 となる場合があることを確認できる。

4. 教育応用：情報セキュリティアンプラグド

現在の情報化社会においては、そこに関わるすべての人々の情報セキュリティへの理解と実践が必須となっている。一方、情報セキュリティは難しいという先入観（学習障壁）をもつ人や、情報セキュリティのために何をすればよいか（情報セキュリティ的思考）が分からないという人も少なくない。本節は、これらの問題点を踏まえ、物理的暗号技術を用いた情報セキュリティ教育の有用性を議論する。

4.1 情報セキュリティ教育の障壁低減

計算機に不慣れな人が計算機科学を学習する上では、計算機を使いこなすことが障壁となる。そのような障壁を下げることを目的として、計算機を使用せずに計算機科学を教育する *Computer Science Unplugged* (CS-Unplugged, [9]) という手法が開発され、教育に活用されている。

現代の情報セキュリティ技術は高度な数学に基づいており、実装には計算機が必須となっている。そのため、情報セキュリティ教育は計算機科学と同様の学習障壁を有している。物理的暗号技術は、そのような学習障壁を取り除くツールであると期待される。実際、文献 [7] は、国内外の大学の事例を紹介し、カードベースプロトコルを教材とした情報セキュリティの教育事例を報告している。このことは、初学者に学習障壁を下げて情報セキュリティ教育を施すことの有効性の傍証といえよう。

また、物理的暗号技術は、身近に存在するカードやコインなどを利用するために、初学者にも親近感をもたせやすい。教育手法としてエデュテインメントが確立しているように、親近感のあるカードなどを使ってゲーム感覚で学習することにより、学習効果が向上することも期待できる。

物理的暗号技術は、視覚的に処理を追跡できるためにプロトコルの原理を直感的に理解しやすい。そのうえ、ブラックボックスとなる計算機を利用しないために、不意の情報漏洩が生じないという安心感がある。世の中に広く普及される暗号技術には、高機能化だけでなく人間への優しさが必要であるとされている [8]。すなわち、物理的暗号技術は、実用性も兼ね備えた情報セキュリティ教育の教材となりうる。

このように、学習障壁を下げることは、初学者に対して有効であるばかりでなく、情報セキュリティは難しいという観念を抱いてしまった社会人に対しても有効である。このように、物理的暗号技術を用いた情報セキュリティ教育は、リカレント教育への応用も期待される。

4.2 情報セキュリティ的思考の養成

情報セキュリティは、機密性や完全性、可用性に対する様々な脅威から情報資産を守ることが基本である。そのためには、守るべき**情報資産**やシステムへの**脅威**、システムの**脆弱性**を特定して**リスク**を分析し、**対策**を立案しなければならない。物理的暗号技術を Toy Example として用いた演習により、そのような情報セキュリティの考え方の学習効果が向上すると期待される。

物理的暗号技術を用いる場合には、**情報資産**はユーザの入力である。入力は予め定められた分布に従って与えられる。例えば、2.1 節で紹介した $\mathcal{P}^{\mathsf{MS}}$ では、入力 $(a,b) \in \{0,1\}^2$ は初期状態の確率トレースに含まれる各確率 p_{ab} に従う。入力が所定の分布に従っていること以上の情報が漏れた場合には、物理的暗号技術を用いたシステムのセキュリティが損なわれたとみなす。

物理的暗号技術を用いるシステムへの**脅威**は、例えば、操作の改竄やミスなどである。3 節では、カードの巡回シフト操作やコインの手渡し操作において、誤りを確率的に表現した。このような表現は、故意（意図的な改竄）と過失（ミス）の双方を包含している。

これらシステムの**脆弱性**は、例えば、誤操作の検出機能の欠如などである。2.1 節で紹介した $\mathcal{P}^{\mathsf{MS}}$ は、正しく AND 計算を実行することを目的として[*2]設計されたプロトコルであり、脅威（誤操作）によってシステムが影響を受ける脆弱性さを有する。あるいは、背面操作（あるユーザが他

[*2] 加えて、計算結果をカードを伏せた状態で導く（コミット型プロトコルという）ことで、計算結果を次のプロトコルの入力として再利用可能な、簡便なプロトコルを実現することも目的としている。

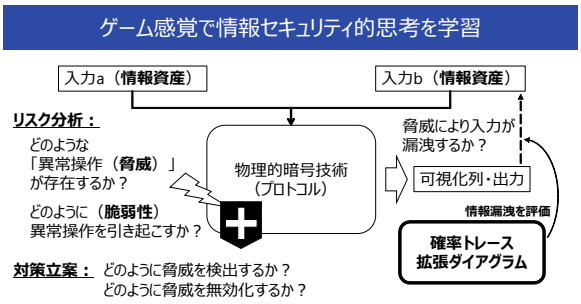

図 5　物理的暗号技術を用いた情報セキュリティ的思考の教育

方のユーザに見えないようにしてカードなどを操作すること）を含むプロトコルは、脆弱性を有すると考えられる。

抽出した脅威や脆弱性に対して、システムのセキュリティが損なわれる**リスク**を分析する。3 節は、誤操作を確率的に表現して、プロトコルの挙動を**確率トレース**と**拡張ダイアグラム**を用いて可視化した。ダイアグラム中の情報漏洩に繋がる事象に着目して、確率を評価（設定）することにより、リスク分析を実践できる。例えば、使用するカードやコインの形状によっては意図的な（手品のような）誤操作を混入させやすい[*3]、背面操作時にも意図的な誤操作を混入させやすい、ために、リスクが高いと考えられる。

脆弱性やリスクに対して、**対策**を立案する。例えば、文献 [5] は、一部のカードの向きを上下逆さまにして誤操作を検出する手法を提案している。

物理的暗号技術の各操作に対して、図 5 に示すように、正常とは異なるふるまいを導くリスク（脅威と脆弱性）や対策を、受講者同士でカードやコインを実際に操作しながら議論する。ゲーム感覚で、相手の入力を推測するための脅威や脆弱性を探索したり、自身の入力を守るための対策を検討したりすることで、学習効果が高まると考えられる。

5. まとめ

本稿は、物理的暗号技術に対して、異常操作を含む変形プロトコルからの情報漏洩の体系的な評価手法を提案し、既存のプロトコルに適用して効果を確認した。さらに、故意や過失による異常処理からの情報漏洩や対策といった、情報セキュリティの考え方の教育への応用可能性を論じた。異常処理からの情報漏洩に耐性のあるプロトコルや、情報セキュリティ教育に適したプロトコルと教材の開発は、今後の課題である。

謝辞. 本研究は JSPS 科研費 17K00001 の助成を受けたものです.

[*3] 例えば、手で隠しやすい小さなカードやコインを用いると、見ている人を騙しやすい。このような場合には、小さなカードやコインを脆弱性の一つとみなすこともできる。

参考文献

[1] den Boer, B.: More efficient match-making and satisfiability: the five card trick. In Quisquater, J.J., Vandewalle, J., eds.: Advances in Cryptology — EUROCRYPT '89. Volume 434 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (1990) 208–217

[2] Koch, A., Walzer, S., Härtel, K.: Card-based cryptographic protocols using a minimal number of cards. In Iwata, T., Cheon, J., eds.: Advances in Cryptology – ASIACRYPT 2015. Volume 9452 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2015) 783–807

[3] Mizuki, T., Shizuya, H.: Computational model of card-based cryptographic protocols and its applications. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **E100.A**(1) (2017) 3–11

[4] Mizuki, T., Sone, H.: Six-card secure AND and four-card secure XOR. In Deng, X., Hopcroft, J.E., Xue, J., eds.: Frontiers in Algorithmics. Volume 5598 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2009) 358–369

[5] Mizuki, T., Komano, Y.: Analysis of information leakage due to operative errors in card-based protocols. In Iliopoulos, C.S., Leong, H.W., Sung, W., eds.: Combinatorial Algorithms - 29th International Workshop, IWOCA 2018. Volume 10979 of Lecture Notes in Computer Science., Springer (2018) 250–262

[6] 駒野 雄一, 水木 敬明: コインを用いる新たなマルチパーティ計算. マルチメディア、分散、協調とモバイル (DICOMO2018) シンポジウム, 2018 年, 2H-2, 441–447

[7] 水木 敬明: カードベース暗号の教育への応用. 信学技報, vol. 116, no. 289, ISEC2016-53, pp.13–17, 2016 年 11 月.

[8] Hanaoka, G.: Towards User-Friendly Cryptography. In Phan, R. C.-W., Yung, M., eds.: Paradigms in Cryptology - Mycrypt 2016. Malicious and Exploratory Cryptology. Volume 10311 of Lecture Notes in Computer Science., Springer (2017) 481–484

[9] Bell, T., Witten, Ian H., Fellows, M.: CS Unplugged: An enrichment and extension programme for primary-aged students. 2015