ブロックサインの安全性に対するコードブックの影響

三澤 裕人 †　　徳重 佑樹 †　　岩本 貢 †　　太田和夫 †

† 電気通信大学
182-8585 東京都調布市 調布ケ丘 1 丁目 5-1
{m.yuto,yuuki.tokushige,mitsugu,kazuo.ohta}@uec.ac.jp

あらまし　ブロックサインは，野球などのスポーツにおいて利用されている，体の部位を触る回数や順序によって，安全に作戦を伝達する方法である．一般的な共通鍵暗号は秘密鍵のみを秘匿していることに対して，ブロックサインの典型的なプロトコルは秘密鍵に加えてコードブックも秘匿しているため，安全だと信じられている．本研究では，ブロックサインの安全性に対するコードブックの影響の理論解析を行う．コードブックを公開した場合と比較して，コードブックを秘匿にすることで，ブロックサインの安全性が向上することを，野球に関するシミュレーションによって示す．

Impact of Code Book on Security of Coded Sign

Yuto Misawa †　　Tokushige Yuuki †　　Mitsugu Iwamoto †　　Kazuo Ohta †

†The University of Electro-Communications.
1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, JAPAN
{m.yuto,yuuki.tokushige,mitsugu,kazuo.ohta}@uec.ac.jp

Abstract　In sports such as baseball, coded sign is used for transmitting operations securely by series of touching the parts of the body. A widely used protocol of coded signs is believed to be secure since both of secret key and code book are kept private, while only a secret key is private in ordinary symmetric key cryptography. Hence, we study the impact of private code books on the security of coded signs from a viewpoint of cryptography. In the case of baseball, our simulation results show how the private code book actually enhances the security of coded sign compared to the one with public code book.

1　はじめに

背景　通常の暗号プロトコルは計算機で計算を行い，計算機同士が通信することで実現される．すなわち，これらの暗号プロトコルは，ある程度の計算資源が利用可能であることを前提に設計されている．一方で，計算機を用いずに人間同士で行う暗号プロトコルの設計は，非常に制限された計算資源のもとで安全性を保証することが求められるため，実用的な観点のみならず，理論的な面からも興味深い．このような，人間による情報処理と通信に基づく暗号プロトコルの設計や安全性検証に関する研究としては，[1–4] などが知られている．しかし，これらの研究は主に理論的な検討にとどまっており，実際のシステムを考察対象とはしていない．さらに，これらの研究成果の多くは人間同士の認証を目的にしており，暗号通信に関する考察は [2] の一部にみられるのみである．

目的　このような背景に基づき，本研究では，実システムとして用いられている人間同士の暗号通信として，野球やアメリカンフットボールで用いられるブロックサインを暗号学的視点で解析することを目標とする．ブロックサインとは，体の部位を触る回数や順序によって，安全に作戦を伝達する方法である．ブロックサインは，生身の人間が暗号化と復号を行うため，方式の容易さと安全性の間にトレードオフが存在する．例えば，漏洩対策のために複雑な計算を要求すれば作戦の伝達ミスが増加し，簡単な方式にすると作戦が漏洩しやすくなる．ブロックサインはプレーヤのレベルに応じて複雑さが異なるが，どの方式も，経験的にこれらのトレードオフがバラ

ンスよく保たれていると考えられるため，暗号学的な観点から考察を加える価値がある．

ブロックサインでは，作戦から体の部位に変換した後，その体の部位に対して，簡易な共通鍵暗号を適用する，といった方式が主流となっている．作戦を体の部位に変換する対応表を本稿ではコードブックと呼ぶ．ブロックサインで利用できる秘密鍵暗号は非常に簡単なものであるため，コードブックを秘匿して秘密鍵の一部とすることで，安全性が高められていることが予想できる．本研究では，コードブックが公開されている場合と，コードブックを非公開にして秘密鍵に含める場合を比較することで，コードブックがブロックサインの安全性にどのように寄与するかを理論的に考察する．

安全性の規準としては，攻撃成功確率に基づく攻撃者のアドバンテージを用い，これによって秘密鍵が安全と考えられるサインの生成可能回数（ライフタイム）を評価する．

成果　著者らは [5] で，ブロックサインに共通して見られる枠組みを共通鍵暗号方式に基づいて定式化し，ブロックサインの安全性を数学的に定義した．この定式化に基づき，野球に用いられる基本的なブロックサインに対して，コードブックを公開した場合の攻撃成功確率を計算し，シミュレーションによる安全性評価を行った．

本稿ではこの安全性評価を拡張し，コードブックを非公開にして秘密鍵に含めたプロトコルに対して最良の攻撃アルゴリズムを提案し，攻撃成功確率を導出する．このプロトコルを，野球に関する現実的なパラメータのもとでシミュレーションし，コードブックが公開されている場合と非公開にして秘密鍵に含める場合での安全性の定量的な比較を行う．その結果，非公開にするコードブックのサイズが大きいほど安全性が向上し，ライフタイムが延びることを明らかにする．

本稿の構成　本稿の 2 節以降の構成は以下の通りである．まず，2 節ではブロックサインの定式化を行い，この定式化に基づき攻撃成功確率を導入することで，アドバンテージの定義を行う．3 節では，本稿で安全性評価を与える方式に対する攻撃成功確率を求め，最良な攻撃手法を提案する．そして，4 節では，コードブックの有無が与える安全性への影響を，シミュレーションにより示す．最後に，5 節でまとめと今後の課題の議論を行う．

2　ブロックサインの定式化

2.1　ブロックサインと共通鍵暗号

ブロックサインとは，体の部位を触る回数や順序によって，安全に作戦を伝達する方法である．この伝達される体の部位の列をサインと呼ぶ．

以下では [5] に従って，サインの生成と取得を暗号化･復号とみなすことで，ブロックサインで共通して用いられる枠組みを共通鍵暗号方式として定式化する．以下では，秘密鍵，作戦（平文），サイン（暗号文）を表す有限集合をそれぞれ $\mathcal{K}, \mathcal{M}, \mathcal{C}$ で標記し，秘密鍵 $k \in \mathcal{K}$ を与えたときの暗号化関数，復号関数をそれぞれ，$\mathrm{Enc}_k(\cdot) : \mathcal{M} \to \mathcal{C}$, $\mathrm{Dec}_k(\cdot) : \mathcal{C} \to \mathcal{M}$ で定める．第 2.3 節で説明する通り，$\mathrm{Enc}_k(\cdot)$ は確率的写像であり，$\mathrm{Dec}_k(\cdot)$ は確定的な写像である．

以上の記法の準備のもとで，ブロックサインのプロトコルは以下の通りとなる．

まず，準備として秘密鍵を共有する．

0. **準備：** 監督と選手は，秘密鍵を $k \xleftarrow{U} \mathcal{K}$ として共有する．

ここで，$\mathcal{K}$ は鍵空間であり，$x \xleftarrow{U} \mathcal{X}$ で有限集合 $\mathcal{X}$ から一様分布に従って，$x \in \mathcal{X}$ が選ばれることを表す．

準備で共有された $k \in \mathcal{K}$ のもとで，ブロックサインを t 回実行する．各 $i = 1, 2, \ldots, t$ 番目のブロックサインの送受信は次のようなプロトコルに従う．以下では i のことを時刻と呼ぶ．

1. **作戦の選択：** 監督は，時刻 i の戦況に従い，作戦 $m^{(i)} \in \mathcal{M}$ を選択する．
2. **サイン生成：** 監督は，暗号化関数を用い，サイン $c^{(i)} = \mathrm{Enc}_k(m^{(i)})$ で得たサイン $c^{(i)} \in \mathcal{C}$ を選手に送信する．
3. **サインの復号：** 選手は，復号関数を用い，作戦 $m^{(i)} = \mathrm{Dec}_k(c^{(i)})$ を得る．
4. **作戦の実行：** 選手は，取得した作戦 $m^{(i)}$ を実行する．

このブロックサインのインタラクションは，図 1 のような暗号プロトコルとなる．

時刻 1 から t までの作戦およびサインの組を

$$m^t := (m^{(1)}, m^{(2)}, \ldots, m^{(t)}) \tag{1}$$

$$c^t := (c^{(1)}, c^{(2)}, \ldots, c^{(t)}) \tag{2}$$

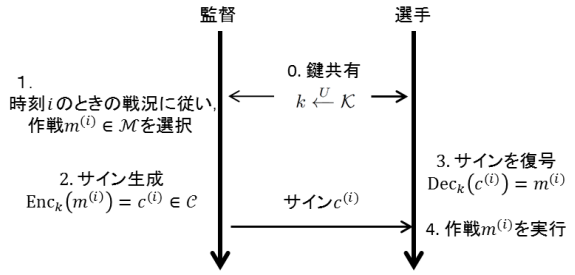

図 1: 時刻 i におけるブロックサインのプロトコル

で定義する．また，サインの組に対する秘密鍵 k による復号を次のように定める．

$$\mathrm{Dec}_k(c^t) := (\mathrm{Dec}_k(c^{(1)}), \ldots, \mathrm{Dec}_k(c^{(t)})) \tag{3}$$

注意 1. 第 2.4 節で述べるように，攻撃成功確率の評価に当たっては，t 回のサインの実行結果を知っている攻撃者が，$t+1$ 回目のサイン（暗号文）を得たときに，作戦（平文）が推測できる確率で定義する．

与えられた秘密鍵 $k \in \mathcal{K}$ に対して，定められた一定の安全性を保ちつつ，パラメータ t を出来るだけ大きくすることが，ブロックサイン作成者の目的となる．この意味で，パラメータ t は秘密鍵のライフタイムと考えることが出来る．

2.2 コードブックと暗号化・復号

実際の野球のブロックサインでは，作戦を体の部位に対応付け，サインとして何度か体の部位を触り，そのいずれかの体の部位が実際に伝えたい作戦である場合が多い．本稿では，上記のようなブロックサインの中でも，何番目かに伝えたい作戦を埋め込む方式に着目する．これを記述するために，ブロックサインに特有の鍵生成法を以下に説明し，$\mathrm{Enc}_k(\cdot)$, $\mathrm{Dec}_k(\cdot)$ の仕様を定める．ここで説明するプロトコルを Π^{BS} と書くことにする．Π^{BS} の概要は図 2 の通りである．

2.2.1 鍵生成

Π^{BS} における秘密鍵はコードブックと，作戦の埋め込み位置から成る．

コードブック 体の部位を表す有限集合を $\mathcal{B}$ とし，作戦を体の部位に対応づける関数を $f : \mathcal{M} \to \mathcal{B}$ と書く．この f を本稿ではコードブックと呼ぶ．本稿では $|\mathcal{M}| = |\mathcal{B}|$ であると仮定し，f は全単射であるとする．そこで，写像 f の集合 $\mathcal{F} \subseteq \mathcal{B}^{\mathcal{M}}$ を次で定義する．

$$\mathcal{F} := \{ f \mid f : \mathcal{M} \to \mathcal{B}, f \text{は全単射} \} \tag{4}$$

作戦の埋め込み位置 ブロックサインで体を触る回数はサインの種類によって異なってよいが，今回は簡単のためにこれを $l \in \mathbb{N}$ で固定する．すると，$\mathcal{C} = \mathcal{B}^l$ と書くことが出来る．長さ l のサインのうち，$p \in [l]$ 番目[1] に真に伝達したい作戦が埋め込まれているとする．

鍵生成では，写像 f と整数 $p \in [l]$ を生成して共有する．すなわち，Π^{BS} における秘密鍵 k は次で定義できる．

$$k := (f, p) \in \mathcal{K} := \mathcal{F} \times [l] \tag{5}$$

注意 2. 通常の暗号では，数値で与えられる秘密鍵そのものが，平文から暗号文への対応を記述するが，ブロックサインにおいては数値としての秘密鍵以外にも，コードブック f も秘匿していることに注意する．f を秘匿することが安全性向上に繋がっていると予想されるため，本稿では，f を秘匿した状況と公開した状況での安全性をそれぞれ理論的に解析し，両者の安全性の比較を行うことが一つの目的である．

2.2.2 暗号化

時刻 i において，秘密鍵 $k = (f, p)$ を与えたときの暗号化 $\mathrm{Enc}_k(\cdot)$ は次のように行われる．

$$\mathrm{Enc}_k(m^{(i)}) = (c_1^{(i)}, c_2^{(i)}, \ldots, c_l^{(i)}) \in \mathcal{B}^l$$
$$\text{where} \begin{cases} c_p^{(i)} = f(m^{(i)}) \\ c_j^{(i)} \xleftarrow{U} \mathcal{B} & \text{if } j \neq p \end{cases} \tag{6}$$

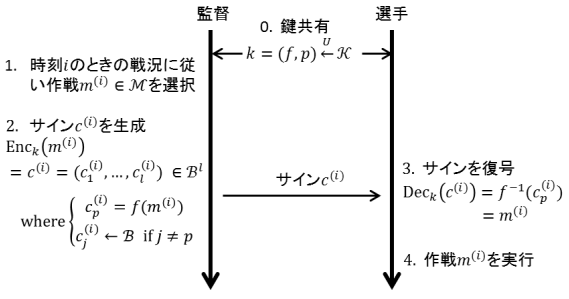

図 2: 時刻 i における Π^{BS} のインタラクション

[1] 自然数 $n \in \mathbb{N}$ に対して，$[n] := \{1, 2, \ldots, n\}$ とする．

表 1: コードブック $f : \mathcal{M} \to \mathcal{B}$ の例

作戦 $\mathcal{M}$	体の部位 $\mathcal{B}$
α	a
β	b
γ	g

2.2.3 復号

復号器の挙動は，上で定めた秘密鍵 $k = (f, p)$ と暗号化関数 $\mathrm{Enc}_k(\cdot)$ の仕様から自然に定まる．すなわち，$c^{(i)} = (c_1^{(i)}, c_2^{(i)}, \ldots, c_l^{(i)})$ から p 番目の要素 $c_p^{(i)}$ を選び，$m^{(i)} = f^{-1}(c_p^{(i)})$ とすれば良い．ここで f^{-1} はコードブック f の逆写像である．

2.2.4 例

サインの長さを $l = 5$ とする．コードブック f を表 1 で定め，作戦の埋め込み位置を $p = 4$ とする．

時刻 i に作戦 $m^{(i)} = \gamma$ を指示するとき，$f(\gamma) = g$ であって $p = 4$ なので，$c_p^{(i)} = g$ とし，残りの b_j は集合 $\mathcal{B}$ から一様分布に従って体の部位を選び，サイン $c^{(i)}$ とする．例えば，$\mathrm{Enc}_{(f,p)}(\gamma) = c^{(i)} = (g, a, b, g, a)$ が出力されたとする．

このとき，選手は共有していた秘密鍵 (f, p) を用いて，$\mathrm{Dec}_{(f,p)}(c^{(i)}) = f^{-1}(c_p^{(i)}) = f^{-1}(g) = \gamma$ とすることで復号できる．

2.3 ブロックサインの確率的定式化

攻撃者の既知平文攻撃に対する攻撃成功確率と，アドバンテージを定義するために，作戦やサインなどの確率分布を定義する．以下では，確率変数を大文字で表記し，その実現地を小文字で表現する．$\mathsf{Pr}\{\cdot\}$ で，括弧内の確率変数に関する同時分布について．括弧内の事象が成立する確率を表す．また，$P_X(x) := \mathsf{Pr}\{X = x\}$ などの記法を用いる．

ブロックサインでは始めに秘密鍵が確率的に選択される．次に，監督は現在の戦況から次に指示する作戦を確率的に選択する．また，暗号化関数も確率的であることに注意する．そこで，秘密鍵，時刻 i $(1 \le i \le t)$ における作戦と暗号文を表す確率変数をそれぞれ，K, $M^{(i)}$, $C^{(i)}$ で定義する．これらの確率変数 K, $M^{(i)}$, $C^{(i)}$ はそれぞれ有限集合 $\mathcal{K}$ $(:= \mathcal{F} \times [p])$, $\mathcal{M}$, $\mathcal{C}$ $(:= \mathcal{B}^l)$ に値を取る．K は $\mathcal{K}$ の一様分布に従い，平文を表す確率変数 $M^{(i)}$, $i = 1, 2, \ldots, t$ とは独立である．また，暗号化関数 $\mathrm{Enc}_k(\cdot)$ の定義から，$k = (f, p)$ が与えられたもとで，次が成り立つ．

$$P_{C^t|K}(c^t|k) = P_{M^t}(\mathrm{Dec}_k(c^t)) \prod_{i=1}^{t} \prod_{\substack{j=1 \\ j \neq p}}^{l} P_{C_j^{(i)}}(c_j^{(i)}) = \frac{P_{M^t}(\mathrm{Dec}_k(c^t))}{|\mathcal{B}^{t(l-1)}|} \tag{7}$$

ここで $C_j^{(i)}$ は $c_j^{(i)}$ に対応する確率変数である．$C^{(i)}$ に関する周辺分布を計算すると次を得る．

$$P_{C^{(i)}|K}(c^{(i)}|(f,p)) = \frac{P_{M^{(i)}}(f^{-1}(c_p^{(i)})}{|\mathcal{B}^{l-1}|} \tag{8}$$

また，復号関数 $\mathrm{Dec}_k(\cdot)$ の構造より，サインと秘密鍵の組 $(c^{(i)}, k)$ に対して作戦 $m^{(i)}$ が一意に対応付けられていることに注意すると，次が成り立つ：

$$P_{M^{(i)}|KC^{(i)}}(m^{(i)}|k, c^{(i)}) = \begin{cases} 1 & \text{if } \mathrm{Dec}_k(c^{(i)}) = m^{(i)} \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

以下では，議論の簡単化のために，二つの仮定を設ける：

仮定 1. 全ての確率変数に関する確率的な依存関係，確率分布は既知である．

仮定 2. サインによって送信された作戦は常に正しく取得され，伝えられた作戦は必ず実行される．

注意 3. 仮定 1 について，確率分布 $P_{M^{(i)}}(m^{(i)})$ は実際には監督が立てる作戦のモデル化であり，攻撃者の考える作戦の確率分布とは必ずしも一致しない．しかし，$P_{M^{(i)}}(m^{(i)})$ は攻撃者にとっても戦況からかなり推定が出来るものと考え，議論の簡単化のためにこのような仮定をおいている．

仮定 2 は，暗号理論における完全復号条件, $\forall k \in \mathcal{K}$, $\mathsf{Pr}\{\mathrm{Dec}_k(\mathrm{Enc}_k(M)) = M\} = 1$ と等価である．実際には，送信された作戦の取得に失敗したり，実行した作戦が失敗することが起こり得るが，第 2.4 節で述べるとおり，この仮定により，ブロックサインに対する攻撃が，既知平文攻撃であると考えることが出来る．

2.4 攻撃成功確率とアドバンテージ

前節の仮定 2 から，攻撃者は時刻 1 から時刻 t までの計 t 回分の過去の作戦，サインの組を観測する

ことができる．そこで攻撃者は，これらの過去 t 回分の過去の作戦，サインの組を用いて，時刻 $t+1$ における新しいサインから次の作戦を予想することができる．この新しいサインをチャレンジと呼び，攻撃者が，過去の観測結果を用いてチャレンジ $c^{(t+1)}$ から正しく作戦 $m^{(t+1)}$ を復号できたときを攻撃成功と定義する．これは，暗号学的には既知平文攻撃ということができる．仮定 1 により，全ての確率変数の依存関係，確率分布は既知であるため，ブロックサインのアドバンテージを定義することができる．

定義 1 (ブロックサインの攻撃成功確率)**.** $|\mathcal{M}| = n$ とサインの長さ l と観測回数 t が与えられた時，攻撃成功確率の上限を次で定義する．

$$\Sigma(n,l;t) := \sum_{\substack{(m^t,c^{t+1}) \\ \in(\mathcal{M}^t,\mathcal{C}^{t+1})}} P_{M^t,C^{t+1}}(m^t,c^{t+1}) \times \max_{\substack{m^{(t+1)} \\ \in\mathcal{M}}} P_{M^{(t+1)}|M^tC^{t+1}}(m^{(t+1)}|m^t,c^{t+1}) \quad (10)$$

過去の作戦とサインやチャレンジを用いない場合に $P_{M^{(t+1)}}(m^{(t+1)})$ のみから得ることができる推測確率の最大値

$$\Gamma(t) := \max_{m^{(t+1)}\in\mathcal{M}} P_{M^{(t+1)}}(m^{(t+1)}) \quad (11)$$

と，定義 1 の攻撃成功確率との差が小さい時，ブロックサインは安全であると考えられる．すなわち，次のように攻撃者のアドバンテージを定義し，その値が十分小さい時に安全であるとする．

定義 2 (攻撃者のアドバンテージ)**.** $|\mathcal{M}| = n$，サインの長さ l，観測回数 t のとき，攻撃者のアドバンテージ $Adv(n,l;t)$ を次で定義する．

$$Adv(n,l;t) := \Sigma(n,l;t) - \Gamma(t) \quad (12)$$

注意 4. このアドバンテージの定義は，[6] で導入された Guessing secrecy を，ブロックサインへの既知平文攻撃に対して，条件付き最小エントロピーを用いずに定義したものである．

3 Π^{BS} の攻撃成功確率と攻撃手法

3.1 過去の情報による秘密鍵の絞り込み

Π^{BS} に対する攻撃成功確率とアドバンテージを評価するために，過去 t 組の作戦とサインの組 (m^t,c^t) を与えて，秘密鍵を絞り込む方法を，$t=2$ の場合に例を用いて説明する．

作戦と体の部位の集合を，$\mathcal{M} = \{\alpha,\beta,\gamma\}$, $\mathcal{B} = \{a,b,g\}$ とする．次に，時刻 1,2 のときのサインと作戦の組をそれぞれ，$c^{(1)} = (a,b,b,a,b)$, $m^{(1)} = \beta$, $c^{(2)} = (g,a,b,a,g)$, $m^{(2)} = \gamma$ とする．f は全単射であることから，$|\mathcal{F}| = 3! = 6$ 通りとなるので，$\mathcal{F} := \{f_1,f_2,\ldots,f_6\}$ とし，各コードブックを表 2 のように定める．

まず，時刻 1 のときの作戦とサインの組 $m^{(1)}, c^{(1)}$ に対する秘密鍵について議論する．コードブックとして f_1 を採用した場合，サインは $c^{(1)} = (\alpha,\beta,\beta,\alpha,\beta)$ となる．このとき，$m^{(1)} = \beta$ であるため，$(f_1,1)$, $(f_1,4)$ は秘密鍵として $(c^{(1)},\ m^{(1)})$ と辻褄が合わず，秘密鍵の候補から外すことが出来る．このように，他のコードブック $f_2,\ldots,f_6$ についても，辻褄が合わない秘密鍵を候補から除外する．結果として時刻 1 で絞り込める秘密鍵の候補の集合として，$\mathcal{K}^{(1)} := \{(f_1,2),(f_1,3),(f_1,5),(f_3,1),(f_3,4),(f_5,1),(f_5,4),(f_6,2),(f_6,3),(f_6,5)\}$ が得られる．さらに，時刻 2 のときの作戦とサインの組 $m^{(2)}, c^{(2)}$ に同様の操作を行い，得られた秘密鍵の候補の集合を $\mathcal{K}^{(2)}$ とすると，過去のサインと作戦 (m^2,c^2) に対する秘密鍵の候補の集合は，$\mathcal{K}^{(1)} \cap \mathcal{K}^{(2)}$ となる．

上記の秘密鍵の絞り込みのように，作戦とサインの組 (m^t,c^t) が与えられた時に，c^t を復号して m^t となるような秘密鍵を出力する関数を次のように定義する．

定義 3. t 個の作戦とサインの組 (m^t,c^t) が得られたときに，これらから絞り込まれる秘密鍵の候補を集めた集合を $\mathcal{K}(m^t,c^t) \subseteq \mathcal{K}$ とする．$\mathcal{K}(m^t,c^t)$ は次のように書ける．

$$\mathcal{K}(m^t,c^t) := \{(f,p)|\forall i \in [t], f(m^{(i)}) = c_p^{(i)}\} \quad (13)$$

このように，過去の情報 (m^t,c^t) を得た攻撃者は，秘密鍵であるコードブック f と作戦の埋め込み位置 p の候補を $\mathcal{K}(m^t,c^t)$ に絞った上で，チャレンジを行うことができる．さらに，仮定 1 により，作戦の

表 2: $|\mathcal{M}| = 3$ の時のコードブック f の集合

	α	β	γ
f_1	a	b	g
f_2	a	g	b
f_3	b	a	g
f_4	b	g	a
f_5	g	a	b
f_6	g	b	a

確率分布を用いることが出来る攻撃者は，$\mathcal{K}(m^t, c^t)$ を用いて攻撃成功確率 $\Sigma(n, l; t)$ を最大化し，結果的に最大のアドバンテージを実現することが出来る．

3.2 節では，$\mathcal{K}(m^t, c^t)$ を用いて Π^{BS} に対する最大攻撃成功確率を導出し，それを達成する攻撃手法を 3.4 節で与える．

3.2 Π^{BS} への最大攻撃成功確率

定義 1 で定めたブロックサイン Π^{BS} に対する最大攻撃成功確率は，チャレンジ時と時刻 1 から時刻 $t+1$ までの作戦の確率分布 $P_{M^{(i)}}(\cdot)$, $i = 1, 2, \ldots, t+1$ と第 3.1 節で導入した集合 $\mathcal{K}(m^t, c^t)$ を用いて次のように書くことが出来る．

定理 1 (Π^{BS} の最大攻撃成功確率)． $|\mathcal{M}| = n$，サインの長さ l，観測回数 t が与えられたとき，Π^{BS} に対する攻撃成功確率 $\Sigma(n, l; t)$ は，次で与えられる．

$$\Sigma(n, l; t) = \frac{1}{n! n^{(t+1)(l-1)} l} \times \sum_{\substack{(m^t, c^{t+1}) \\ \in (\mathcal{M}^t, \mathcal{C}^{t+1})}} \max_{\substack{m^{(t+1)} \\ \in \mathcal{M}}} |\mathcal{K}(m^{t+1}, c^{t+1})| P_{M^{t+1}}(m^{t+1}) \tag{14}$$

定理 1 の証明には，次の 2 つの補題を用いる．紙面の都合上，各補題の証明は省略する．

補題 1. t 個の作戦とサインの組を (m^t, c^t) としたとき，秘密鍵 $k = (f, p) \in \mathcal{K}$ に対して，次式が成立する．

$$P_{K|M^t C^t}(k|m^t, c^t) = \begin{cases} |\mathcal{K}(m^t, c^t)|^{-1} & \text{if} \quad k \in \mathcal{K}(m^t, c^t) \\ 0 & \text{otherwise} \end{cases} \tag{15}$$

補題 2. t 個の作戦とサインの組 (m^t, c^t) およびチャレンジ $c^{(t+1)}$ に対して，次が成り立つ．

$$P_{M^{(t+1)}|M^t C^{t+1}}(m^{(t+1)}|m^t, c^{t+1}) = \frac{|\mathcal{K}(m^{t+1}, c^{t+1})|}{|\mathcal{B}|^{l-1}} \times \frac{P_{M^{(t+1)}|M^t}(m^{(t+1)}|m^t)}{\sum_{k \in \mathcal{K}(m^t, c^t)} P_{C^{(t+1)}|KM^t C^t}(c^{(t+1)}|k, m^t, c^t)} \tag{16}$$

定理 1 の証明： 定義 1 式 (10) における総和の第一項 $P_{M^t C^{t+1}}(m^t, c^{t+1})$ は次のように変形できる．

$$\begin{aligned} &P_{M^t C^{t+1}}(m^t, c^{t+1}) \\ &= P_{C^{(t+1)}|M^t C^t}(c^{(t+1)}|m^t, c^t) P_{C^t}(c^t) \times P_{M^t|C^t}(m^t|c^t) \\ &\overset{(a)}{=} P_{C^{(t+1)}|M^t C^t}(c^{(t+1)}|m^t, c^t) P_{C^t}(c^t) \times \sum_{k \in \mathcal{K}} P_{M^t|KC^t}(m^t|k, c^t) P_{K|C^t}(k|c^t) \\ &\overset{(b)}{=} P_{C^{(t+1)}|M^t C^t}(c^{(t+1)}|m^t, c^t) \times P_{C^t}(c^t) \sum_{k \in \mathcal{K}(m^t, c^t)} P_{K|C^t}(k|c^t) \end{aligned} \tag{17}$$

等号 (a) は全確率の公式，等号 (b) は式 (9) から成り立つ．

次に，式 (17) の各項を評価する．まず，第一項は，次のように変形できる．

$$\begin{aligned} &P_{C^{(t+1)}|M^t C^t}(c^{(t+1)}|m^t, c^t) \\ &= \sum_{k \in \mathcal{K}} P_{C^{(t+1)}|KM^t C^t}(c^{(t+1)}|k, m^t, c^t) \times P_{K|M^t C^t}(k|m^t, c^t) \\ &= |\mathcal{K}(m^t, c^t)|^{-1} \times \sum_{k \in \mathcal{K}(m^t, c^t)} P_{C^{(t+1)}|KM^t C^t}(c^{(t+1)}|k, m^t, c^t) \end{aligned} \tag{18}$$

最後の等号は，補題 1 より導ける．

また，式 (17) の残りの項は次のようになる．

$$\begin{aligned} &P_{C^t}(c^t) \sum_{k \in \mathcal{K}(m^t, c^t)} P_{K|C^t}(k|c^t) \\ &= \sum_{\substack{k=(f,p) \\ \in \mathcal{K}(m^t, c^t)}} P_{C^t|K}(c^t|k) P_K(k) \\ &\overset{(a)}{=} \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}(m^t, c^t)} P_{C^t|K}(c^t|k) \\ &\overset{(b)}{=} \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}(m^t, c^t)} \frac{1}{|\mathcal{B}|^{t(l-1)}} P_{M^t}(m^t) \\ &= \frac{|\mathcal{K}(m^t, c^t)|}{|\mathcal{K}||\mathcal{B}|^{t(l-1)}} P_{M^t}(m^t) \end{aligned} \tag{19}$$

等号 (a), (b) はそれぞれ，K の一様性と，式 (7) より導ける．

したがって $P_{M^t C^{t+1}}(m^t, c^{t+1})$ は，式 (17) に式

(18), (19) を代入すると次のようになる．

$$P_{M^tC^{t+1}}(m^t,c^{t+1}) = \frac{1}{|\mathcal{K}||\mathcal{B}|^{t(l-1)}}P_{M^t}(m^t) \times \sum_{k\in\mathcal{K}(m^t,c^t)} P_{C^{(t+1)}|KM^tC^t}(c^{(t+1)}|k,m^t,c^t) \quad (20)$$

最後に，補題 2 の式 (16) を $m^{(t+1)}$ について最大値をとり，式 (20) とあわせて式 (10) に代入して，次を得る．

$$\begin{aligned}&\Sigma(n,l;t)\\ &= \sum_{\substack{(m^t,c^{t+1})\\ \in(\mathcal{M}^t,\mathcal{C}^{t+1})}} \frac{1}{|\mathcal{K}||\mathcal{B}|^{(t+1)(l-1)}}P_{M^t}(m^t)\\ &\times \max_{\substack{m^{(t+1)}\\ \in\mathcal{M}}} |\mathcal{K}(m^{t+1},c^{t+1})|P_{M^{(t+1)}|M^t}(m^{(t+1)}|m^t)\\ &= \frac{1}{n!n^{(t+1)(l-1)l}}\\ &\times \sum_{\substack{(m^t,c^{t+1})\\ \in(\mathcal{M}^t,\mathcal{C}^{t+1})}} \max_{\substack{m^{(t+1)}\\ \in\mathcal{M}}} |\mathcal{K}(m^{t+1},c^{t+1})|P_{M^{t+1}}(m^{t+1})\end{aligned} \quad (21)$$

以上により，式 (14) が導かれた． □

3.3 コードブックを公開したときの Π^{BS} の攻撃成功確率

コードブックを公開した場合について，定義 3 の関数を，$\mathcal{K}'(m^t,c^t) := \{p|\forall i\in[t], c_p^{(i)} = m^{(i)}\} \subseteq \mathcal{K}$ と定義することで，定理 1 と同様の議論を進めることができる．したがって，コードブックを公開した場合の Π^{BS} を $\Pi^{\mathrm{BS}'}$ とし，その攻撃成功確率は次のようになる．

定理 2 ($\Pi^{\mathrm{BS}'}$ の攻撃成功確率)． $|\mathcal{M}| = n$，サインの長さ l，観測回数 t が与えられたとき，$\Pi^{\mathrm{BS}'}$ に対する攻撃成功確率 $\Sigma'(n,l;t)$ は，次で与えられる．

$$\Sigma'(n,l;t) = \frac{1}{n^{(t+1)(l-1)l}} \times \sum_{\substack{(m^t,c^{t+1})\\ \in(\mathcal{M}^t,\mathcal{C}^{t+1})}} \max_{\substack{m^{(t+1)}\\ \in\mathcal{M}}} |\mathcal{K}'(m^{t+1},c^{t+1})|P_{M^{t+1}}(m^{t+1})$$

注意 5. $\Sigma(n,l;t)$ と比較すると，$\Sigma'(n,l;t)$ には $1/n!$ の項がなく，また鍵の絞り込みを行う関数が $\mathcal{K}'(\cdot,\cdot)$ に置き換わっていることに注意する．すなわち，関数 $\mathcal{K}(\cdot,\cdot),\mathcal{K}'(\cdot,\cdot)$ の違いはあるが，作戦の要素数 n が大きく攻撃成功確率に影響することが予想される．

表 3: 作戦の確率分布

	$t-2$	$t-1$	t	$t+1$
$P_{M^{(i)}}(\alpha)$	0 (0)	($\frac{1}{3}$) $\frac{1}{3}$	0 (0)	$\frac{1}{2}$ ($\frac{1}{4}$)
$P_{M^{(i)}}(\beta)$	0 ($\frac{1}{4}$)	0 (0)	$\frac{1}{4}$ ($\frac{1}{8}$)	0 (0)
$P_{M^{(i)}}(\gamma)$	$\frac{1}{2}$ ($\frac{1}{2}$)	0 ($\frac{1}{6}$)	$\frac{3}{4}$ ($\frac{3}{4}$)	$\frac{1}{2}$ ($\frac{1}{2}$)
$P_{M^{(i)}}(\delta)$	$\frac{1}{2}$ ($\frac{1}{4}$)	$\frac{2}{3}$ ($\frac{1}{2}$)	0 ($\frac{1}{8}$)	0 (0)
$P_{M^{(i)}}(\zeta)$	− (0)	− (0)	− (0)	− ($\frac{1}{4}$)

3.4 攻撃手法

3.2 節では，Π^{BS} の攻撃成功確率を理論的に導出した．この結果から，Π^{BS} に対する各時刻の作戦の確率分布を含めた最良の攻撃は以下のようになる．

1. 取得した過去の情報 (m^t,c^t) とチャレンジ $c^{(t+1)}$ を用いて，各作戦 $m^{(t+1)}\in\mathcal{M}$ について，$|\mathcal{K}(m^{t+1},c^{t+1})|$ を計算する．
2. 各作戦 $m^{(t+1)}$ で，計算した $|\mathcal{K}(m^{t+1},c^{t+1})|$ と $P_{M^{(t+1)}|M^t}(m^{(t+1)}|m^t)$ で積を取り，最大となる作戦 $m^{(t+1)}$ を攻撃者は選択する．

また，$\Pi^{\mathrm{BS}'}$ に対する最良の攻撃手法は，上記の攻撃手法の $\mathcal{K}(\cdot,\cdot)$ を $\mathcal{K}'(\cdot,\cdot)$ に置き換えれば良い．

4 コードブックの安全性への影響

アドバンテージのシミュレーション 定理 1，2 を用いて，Π^{BS} のコードブックが公開の場合と非公開の場合について，現実的なパラメータを与えた時の攻撃者のアドバンテージの評価を行う．また，評価を簡単にするために，作戦の確率変数 $M^{(i)}$ $(1\le i\le t)$ が互いに独立であるとする．

作戦の要素数 $n=4,5$，サインの長さ $l=3$，観測回数 $t=0,1,2,3$ として，シミュレーションを行う．また，各時刻における監督の決める作戦の確率分布を表 3 とする．表の見方は，左の値が $n=4$ の場合，右の丸括弧がついた値が $n=5$ の場合の確率分布となっている．

ここで，チャレンジは時刻 $t+1$ において行うことに注意する．すなわち，$t=3$ のときは攻撃者が最も古い時刻 $t-2$ からサインと作戦を観測しており，$t=2,t=1$ のときも同様にそれぞれ時刻 $t-1$，時刻 t から観測している．また，$\Gamma(t) = P_{M^{(t+1)}}(\gamma) = 1/2$ である．定義 2 より，このときの次の値を求めるこ

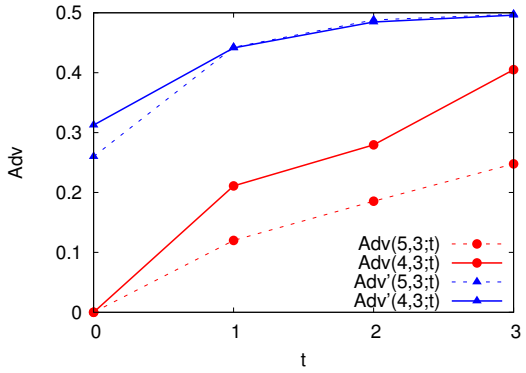

図 3: アドバンテージのグラフ

とで，Π^{BS}，$\Pi^{\mathrm{BS}'}$ それぞれに対するアドバンテージの推移を得る．

$$Adv(n,3;t) = \Sigma(n,3;t) - 1/2$$
$$Adv'(n,3;t) = \Sigma'(n,3;t) - 1/2$$
$$\text{where } n = 4,5,\ t = 0,1,2,3$$

計算機によるシミュレーションを行った結果，アドバンテージと観測回数の関係は図 3 となった．

考察　次の事実より，コードブックのサイズが大きいほど安全性が向上し，秘密鍵のライフタイムが伸びることが確認できる：

- 観測回数が $t = 0$ を除き，$Adv(4,3;t)$ と $Adv(5,3;t)$ の差が 0.09 から 0.15 となっている．
- 観測回数 $t = 2$ の時点で $Adv'(n,3;2)$ が最大のアドバンテージである 0.5 に近い値を取っているのに対し，さらに観測回数を増やした $t = 3$ で $Adv(4,3;3)$ は 0.4，$Adv(5,3;3)$ は 0.25 程度の値となっている．

5　まとめと今後の課題

本稿では，野球に用いられるブロックサインの一つに対して，コードブックが非公開の場合と公開の場合に分けて攻撃成功確率を導出し，最良の攻撃アルゴリズムを提案し，さらに，現実的なパラメータを用いた具体的なシミュレーションを行った．これらの結果から，コードブックを公開，非公開にした場合の両者の安全性を比較することで，コードブックの安全性への影響を議論した．

今後の課題は，他の現実のブロックサインの方式に対して安全性を評価することで，今回評価した方式との比較し，コードブックの影響度合いを調査することがあげられる．

謝辞： 本研究の一部は JSPS 科研費 基盤研究 (B) 15H02710 の助成を受けている．

参考文献

[1] Hopper, N. and Blum, M.: Secure Human Identification Protocols, *Advances in Cryptology–ASIACRYPT 2001* (Boyd, C., ed.), Lecture Notes in Computer Science, Vol. 2248, Springer Berlin Heidelberg, pp. 52–66 (2001).

[2] Matsumoto, T.: Human-computer Cryptography: An Attempt, *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, CCS '96, New York, NY, USA, ACM, pp. 68–75 (1996).

[3] Matsumoto, T. and Imai, H.: Human Identification Through Insecure Channel, Advances in Cryptology–EUROCRYPT '91 (Davies, D., ed.), Lecture Notes in Computer Science, Vol. 547, Springer Berlin Heidelberg, pp. 409–421 (1991).

[4] 松本勉，久保田浩美，井上拓也，鴨志田昭輝，林修一，井上信吾，清水健介：耐クローン性に基づく認証方式の提案，暗号と情報セキュリティシンポジウム 1997，電子情報通信学会，10 pages (1997). 19C.

[5] 三澤裕人，徳重佑樹，岩本貢，太田和夫：簡易なブロックサインに対する暗号理論的安全性解析，暗号と情報セキュリティシンポジウム 2015，電子情報通信学会，8 pages (2015). 3F4-4.

[6] Alimomeni, M. and Safavi-Naini, R.: Guessing Secrecy, *Information Theoretic Security* (Smith, A., ed.), Lecture Notes in Computer Science, Vol. 7412, Springer Berlin Heidelberg, pp. 1–13 (2012).