結託耐性符号の雑音による影響解析

門田　宜也　　栗林　稔　　森井　昌克

神戸大学大学院工学研究科
657-8501 神戸市灘区六甲台町 1-1

nobuya_m@stu.kobe-u.ac.jp　{kminoru,mmorii}@kobe-u.ac.jp

あらまし　Tardos 符号は c-secure 符号の具体的な構成法の一つであり, マーキング仮定を満たすとき理論的な下限に近い符号長で c-secure 符号を実現することが判明している. しかし, 実環境では雑音によりマーキング仮定を満たさない場合があり, 結託耐性の評価としては不十分であった. 本稿では不正符号語に白色雑音を付加し検出を行うことで雑音による結託耐性に対する影響を解析し, マーキング仮定を満たさない場合の Tardos 符号の結託耐性の評価を行う. 結果, 雑音のある通信路上での結託者の相関値の確率密度関数の導出に成功した. また, 雑音により誤検出が増加するため, 従来の閾値の決定方法では不十分であることが明らかになった.

The Performance of Fingerprinting Codes over AWGN Channel

Nobuya Monden　　Minoru Kuribayashi　　Masakatu Morii

Graduate School of Engineering, Kobe University
1-1, Rokkodai, Nada-ku, Kobe-shi, 657-8501, Japan

nobuya_m@stu.kobe-u.ac.jp　{kminoru,mmorii}@kobe-u.ac.jp

Abstract　Tardos's fingerprinting code is a kind of c-secure code which code length is theoretically minimum order under the Marking Assumption. In practical cases, however, the assumption is not always valid because a noise injected through AWGN Channel will flip some bits. In this study, we analyze the performance of Tardos's Codes over AWGN Channel. First, the probability density function of the colluders' correlation score is derived when Gaussian noise is added. Then, we show that the false positive detection increases linearly to the number of flipped bits, which implies that the decision of a threshold is not valid under the noisy channel.

1　はじめに

近年, インターネットの普及によりディジタルコンテンツの不正配布が問題となっている. コンテンツに人間には知覚できないようにユーザ ID を埋め込むことで, 不正配布を行ったユーザを特定する電子透かしという技術がある. 電子指紋技術では同じコンテンツにユーザごとに異なる ID 情報を埋め込む. そのため, 複数の不正ユーザが結託して, 埋め込まれている ID 情報を検知できないように改ざんされる恐れがある. この結託に対し耐性を持つ符号として, Boneh と Shaw は結託耐性符号 (c-secure 符号 [1]) を提案した. c-secure 符号とは, c 人以下の結託に対して誤り確率 ϵ 以下で不正者の追跡を行うことができる符号である. Tardos 符号 [2] は, c-secure 符号の具体的な構成法の一つであり, 理論的な下限に近い符号長で, c-secure 符号を実現できることが判明している [3]. しかし, この評価はマーキング仮定を満たす場合であり, 雑

音が付加される実環境での性能評価としては不十分であった.

本稿では, 不正符号語に白色ガウス雑音を付加することで, マーキング仮定を満たさない場合の Tardos 符号の結託耐性の評価と理論的解析を行う. シミュレーションと解析の結果, 不正者の相関値の確率密度関数を導出し, 雑音のある通信路を経由した不正コピーから結託者を検出できる確率を求める. また, 雑音によるビット反転が増加するに従い, 誤検出がどのように変化するかを実験的に確認する. この結果から AWGN 通信路上では従来の閾値の設定方法 [6] では誤検出が設定以上に起こることを示す.

2 関連研究

本章では, c-secure 符号について, Tardos 符号の構成法, 追跡アルゴリズム, 及び閾値の設定法について述べる. また, 従来結託者が不正符号語を構成する場合に満たす要件とされていたマーキング仮定について述べる.

2.1 c-secure 符号

シンボル Σ 上の符号長 L, ユーザ数 N のフィンガープリント符号 $X : N \times L$ 行列が, 告発アルゴリズム σ を用いたとき, 結託者数 $c' = |C| \leq c$ のどのような $C \subseteq [N] = \{1, 2, \cdots, N\}$, どのような C-strategy ρ に対しても

$$\Pr[\sigma(\rho(X)) = \emptyset \vee \sigma(\rho(X)) \not\subseteq C] \leq \epsilon \quad (1)$$

を満たすとき c-secure 符号という. c-secure 符号には, 二つの誤り確率があり

false positive 率 (誤検出が起こる確率)

$$\epsilon_p = \Pr[\sigma(\rho(X)) \neq \emptyset \cap \sigma(\rho(X)) \notin C]$$

false negative 率 (結託者を一人も検出できない確率)

$$\epsilon_n = \Pr[\sigma(\rho(X)) = \emptyset]$$

と定義される. また, C-strategy ρ は以下のように定義される.

C-strategy ρ

$\emptyset \neq C \in [n]$ に対して以下のように定義された攻撃アルゴリズムである.

入力:X のうち C に属するユーザ符号の列から構成される X の部分行列 X'

出力:$y = \rho(X') \in \Sigma^L$

マーキング仮定:j 番目の結託者の符号語の i 番目のシンボルを $X'_j = (X'_{j1}, \cdots, X'_{jL})(1 \leq j \leq c')$ として, $X'_{1i}, \cdots, X'_{c'i}$ が一致する場合, 結託符号語の i 番目のシンボル y_i は結託者の符号語に一致する.

2.2 Tardos 符号

符号長 L, ユーザ数 N, 誤り確率 ϵ, 結託耐性上限を c 人として, 特に $L = 100ck$, $k = \ln\lceil N/\epsilon \rceil$ を満たすとき, 以下のように Tardos 符号が構成される.

1. コンテンツ配布者はある連続型の確率分布 P に従って, $p_i (1 \leq i \leq L)$ を独立に選び, 列 $P = (p_1, ..., p_L)$ を秘密に保持しておく. ここで P_i は以下を満たすものとする. また, r_i は $[t', \pi/2 - t']$ においてランダムに選ばれる.

$$\begin{cases} t = 1/(300c) \\ 0 < t' < \pi/4, \sin^2 t' = t, r_i \in [t', \pi/2 - t'] \\ p_i = \sin^2 r_i, t \leq p_i \leq 1 - t \end{cases} \quad (2)$$

2. j 番目のユーザ u_j の符号語 $X_j = (X_{ji}, ..., X_{jL})$ を $\Sigma = \{0, 1\}$ から $\Pr(X_{ji} = 1) = p_i$ で確率的に選ぶ.

2.3 追跡アルゴリズム

不正コンテンツから抽出された不正符号語を $y = (y_1, ..., y_L)$, $y_i \in \{0, 1\}$ とする. 本稿では, Škorić らにより示された手法 [3] により各ユーザ符号語と不正符号語の相関値 S_j を求める. Škorić らの手法は, 相関値の計算方法に改良を加えることで従来提案されていた Tardos 符号より高い結託耐性を実現している. 相関値 S_j について以下に示す.

$$S_j = \sum_{i=1}^{L} (2y_i - 1) U_{ji}$$

$$U_{ji} = \begin{cases} \sqrt{\frac{1-p_i}{p_i}} & (X_{ji}=1) \\ -\sqrt{\frac{p_i}{(1-p_i)}} & (X_{ji}=0) \end{cases} \quad (3)$$

相関値 S_j が閾値 Z を超えるユーザ u_j を不正ユーザとして告発する.

2.4 正規分布を利用した閾値の設定法

Tardos 符号における相関値 S_j の確率密度関数は中心極限定理により, 正規分布に近似できる.

定理 2.1 (中心極限定理) 確率変数 $a_1, \ldots, a_n$ が互いに独立で, 平均 μ, 分散 σ^2 の分布に従うとする. n が大きい場合, 各確率変数の和の分布は平均 $n\mu$, 分散 $n\sigma^2$ の正規分布に近似できる.

結託者数が c' 人のとき, 正規ユーザの各ビットの相関値の確率密度関数は平均 0, 分散 1 となることが知られている [4]. Tardos 符号において各ビットは互いに独立であり, 符号長 L が十分大きいため, 中心極限定理より正規ユーザの相関値の確率密度関数は平均 0, 分散 L の正規分布に近似できる.

結託者の各ビットの相関値の結託者の各ビットの相関値の確率密度関数は平均 $2/c'\pi$, 分散 $(1-\frac{4}{(c'\pi)^2})$ の分布となることが知られている. 正規ユーザの場合と同様に, 結託者の相関値の確率密度関数は中心極限定理より, 平均 $\mu(L,c') = 2L/c'\pi$, 分散 $\sigma^2(L,c') = L(1-\frac{4}{(c'\pi)^2})$ の正規分布に近似できる.

また, 平均 0, 分散 σ^2 の正規分布となる確率変数 X が x 以上となる確率 $\Pr[X > x]$ は次の式で表せる.

$$\Pr[X > x] = \frac{1}{2}\mathrm{erfc}\left(\frac{x}{\sqrt{2\sigma^2}}\right) \quad (4)$$

式 (4) を用いることで図 1 に示すように, ユーザ一人当たりの false positive 率 ϵ_p に応じた閾値 Z を決定することができる.

3 結託者の相関値分布の解析

本章では, 雑音によってビット反転が起こる場合の結託者の相関値の分布について評価を行う. 最初に x ビットが反転した場合の結託者の相関値の分布について理論的解析を行い, 次に n[dB] の白色雑音を加えた場合に x ビットが反転する確率について述べる. 最後に雑音と結託者の相関値の分布の関係について解析を行う.

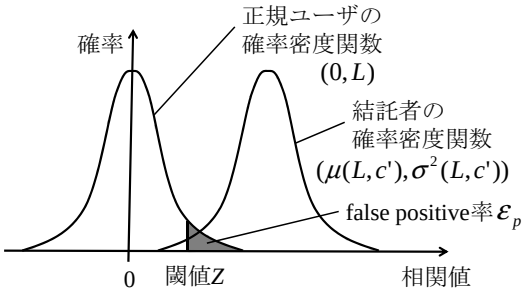

図 1: 閾値の設定

3.1 結託者の相関値

最初に, 1 ビットの反転が結託者の相関値の分布に与える影響を述べ, 次に x ビットが反転した場合の結託者の相関値について述べる. i 番目のビット y_i が反転した場合, 関係するスコア S'_{ji} は式 (3) より以下のように表せる.

$$S'_{ji} = (2\overline{y}_i - 1)U_{ji} = -S_{ji} \quad (5)$$

ただし, $\overline{y}_i$ は y_i が反転したものとする. ビット反転によって, 全てのユーザの相関値の正負が入れ替わるため, 相関値の分散は変化しない. 結託者の各ビットの相関値の確率密度関数は, 通常平均 $2/c'\pi$, 分散 $(1-\frac{4}{(c'\pi)^2})$ であるため, ビット反転した場合, 平均 $-2/c'\pi$, 分散 $(1-\frac{4}{(c'\pi)^2})$ となる.

x ビットが反転した場合に符号語全体で結託者の相関値がどのように分布するか考える. 全ビットの相関値の分散が等しく L が十分大きいため, 符号語全体の相関値の確率密度関数は中心極限定理を用いて以下の平均 μ', 分散 σ' の正規分布として表せる.

$$\begin{aligned} \mu' &= \mu((L-x),c') - \mu(x,c') \\ &= \frac{2(L-2x)}{c'\pi} \quad (6) \\ \sigma'^2 &= \sigma^2(L,c') = L\left(1-\frac{4}{(c'\pi)^2}\right) \quad (7) \end{aligned}$$

x ビット反転した場合の結託者の相関値の確率密度関数を以降 PDF(x) と表記する．雑音によるビット反転数に応じて結託者の相関値の平均は小さくなるが, ビット反転が起こっても分散は変化しないことがわかる．

3.2 ビット反転数

結託符号語が AWGN 通信路を経由して通信された場合に反転するビット数について述べる． ビット反転数は信号に対する雑音の大きさ (SNR) によって定まる． 本稿では, シンボル “0”, “1” で構成される不正符号語 y を “+1”, “−1” の BPSK の信号 Y に対応させて伝送する場合を考える．信号 Y に通信路上の雑音として n[dB] の白色雑音を付加, 受信し, 信号電圧 “0” を境界にディジタル化 (復号) を行うものとする．信号電力を P_S, 雑音電力を P_N とすると SNR は以下のように表せる．

$$\mathrm{SNR} = 10\log_{10}\frac{P_S}{P_N} \tag{8}$$

信号電圧が “+1”, “−1” であるので, P_S は

$$P_S = L \tag{9}$$

SNR=n[dB] のときの雑音の分散を σ_n^2 とすると,

$$P_N = \sum^{L}\sigma_n^2 = \sigma_n^2 L \tag{10}$$

となる．式 (8), (9), (10) より, SNR=n[dB] に対する σ_n^2 が定まる．式 (4) より, あるビットが反転する確率を p_n は σ_n^2 を用いて以下のように求めることができる．

$$\begin{aligned} p_n &= \sum_{i=1}^{L}\Pr(Y_i=-1)\frac{1}{2}\mathrm{erfc}\left(\frac{1}{\sqrt{2\sigma_n^2}}\right) \\ &\quad +\sum_{i=1}^{L}\Pr(Y_i=1)\frac{1}{2}\left(1-\mathrm{erfc}\left(\frac{-1}{\sqrt{2\sigma_n^2}}\right)\right) \\ &= \frac{1}{2}\mathrm{erfc}\left(\frac{1}{\sqrt{2\sigma_n^2}}\right) \end{aligned} \tag{11}$$

符号長 L において x ビットが反転する確率は, σ_n^2 を用いて以下のような二項分布として表せる．

$$P(x) = {}_L\mathrm{C}_x p_n^x (1-p_n)^{L-x} \tag{12}$$

ビット反転数の期待値は,

$$\begin{aligned} E(X) &= \sum_{x=0}^{L} xP(x) \\ &= Lp_n\sum_{x=1}^{L}{}_{n-1}\mathrm{C}_{x-1}p_n^{x-1}(1-p_n)^{L-x} \\ &= Lp_n \end{aligned} \tag{13}$$

となり, 分散値は,

$$\begin{aligned} V(X) &= E(X^2)-(E(X))^2 \\ &= E(X(X-1))+E(X)-(E(X))^2 \\ &= L(L-1)p_n^2+Lp_n-(Lp_n)^2 \\ &= Lp_n(1-p_n) \end{aligned} \tag{14}$$

となる．ここで符号長 L は十分に大きいため, 中心極限定理より, 雑音が n[dB] のとき x ビットが反転する確率密度関数 $P(x)$ は平均 Lp_n, 分散 $Lp_n(1-p_n)$ の正規分布に近似することができる．

3.3 雑音と結託者の相関値の分布の関係

3.1 節, 3.2 節で, ビット反転数が x ビットの場合の結託者の分布 PDF(x) と x ビットが反転する確率 $P(x)$ を導出した．雑音が n[dB] のとき, 結託者が相関値 s をとる確率密度関数は以下のように表すことができる．

$$g(s) = \sum_{k=0}^{L}(\mathrm{PDF}(k)\times P(k)) \tag{15}$$

式 (15) により, AWGN 通信路を経由した結託符号語から結託者が検出される確率を求めることができる．

4 正規ユーザの相関値分布の解析

文献 [4] によると, 正規ユーザの相関値の確率密度関数はどのような符号語と相関値を求めても平均 0, 分散 L の正規分布となることが知られている．ゆえにビット反転によって, マーキング仮定を満たさない場合でも正規ユーザの相関値の確率密度関数も正規分布に近似が行えると考えられる．本稿では実際にシミュレーションを行うことで, 2.4 節に示す方法で設定を行った閾値に対する false positive 率を調べる．

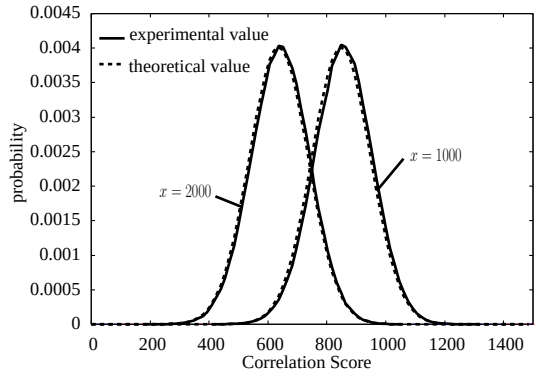

図 2: x ビット反転時の結託者の相関値の確率分布

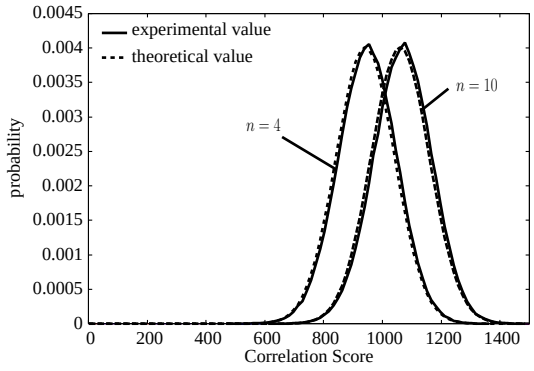

図 3: n[dB] での結託者の相関値の確率分布

5 シミュレーション結果・考察

本章では結託者と正規ユーザについてシミュレーションを行った環境とその結果について示し, その考察を行う.

5.1 結託者について

雑音によって x ビットが反転した場合の結託者の相関値シミュレーションを 10^6 回行い, 式 (15) で導出した理論値との比較を行った. 本稿のシミュレーションは全て結託攻撃として符号語の各シンボルを結託者内で最も多いシンボルに書き換える Majority Attack を用いて行った. 結果を図 2 に示す. シミュレーション環境は $L = 10^4$, 結託耐性上限 $c = 20$, 結託者数 $c' = 4, 6$, $Z = 561(\epsilon_p{=}10^{-8})$, $x = 1000, 2000$ である. 図 2 より, 理論値がシミュレーション結果と一致し, 理論値が正しいことがわかる.

また, n[dB] の雑音通信路上での結託者の相関値シミュレーションを 10^6 回試行し, 式 (15) の理論値を比較した. 結果を図 3 に示す. シミュレーション環境は $L = 10^4$, $c = 20$, $c'{=}6$, $n{=}4, 10$ である. 理論値とシミュレーション結果が一致し, 理論値が正しいことがわかる. また, 雑音が大きいほど結託者の相関値が小さくなる. これは 3.2 節に示されたように雑音が大きいほど反転ビット数が増加し, それに伴い 3.1 節に示すように結託者の平均値が下がるためである.

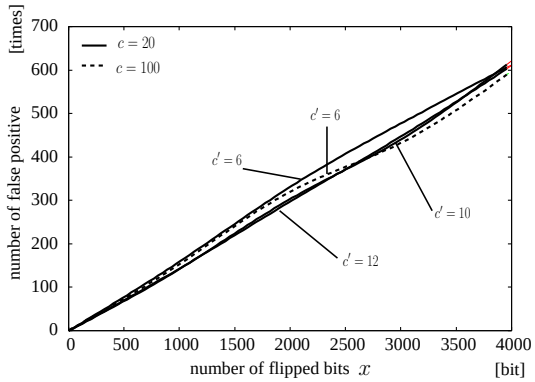

図 4: ビット反転数と誤検出回数の関係

5.2 正規ユーザについて

$L = 10^4$, $Z = 561(\epsilon_p{=}10^{-8})$, ユーザ数 $N = 10^4$ において, x ビット反転した場合の正規ユーザの相関値の分布についてシミュレーションを行った. 実験環境は x=0, 1000, 2000, 3000, 4000, $c = 20$, c'=6, 10, 12 と $c = 100$, $c' = 6$ で 10^4 回試行した. 従来示されていた通り平均, 分散はほとんど変化しなかったが, ビット反転によって, 誤検出が大きく増加することがわかった. 誤検出回数とビット反転数のシミュレーション結果を図 4 に示す.

反転ビット数が増えるにつれ, 誤検出回数が線形的に増加している. 反転ビット数 x と誤検出回数 f_p の関係は $f_p = \sqrt{2}x$ 程度であった. 正規ユーザの分布は一見変わらないが, ごく少数の正規ユーザがビット反転により, 大きな相関値をとるため誤検出が起こる. これは p_i が 0 もしくは 1 に近い値をとる i 番目のビットが反転

した場合に, 式 (3) によって与えられる相関値がごく少数の正規ユーザにおいて大きな値になることが理由と考えられる．また, 誤検出回数の増加は確率分布 P によって変化すると考えられるが $c = 20,100$ において大きな変化がないため, 実用的な範囲では c に対する依存性は小さいと考えられる．AWGN 通信路上では, 3.2 節に示したように雑音が大きければ反転ビット数も増加する．そのため, 雑音によるビット反転が起こる環境において確率分布が正規分布となることを利用した従来の閾値の設定法を用いると, 誤検出回数が増加する.

6 まとめ

本稿では, 雑音によってマーキング仮定を満たさない場合の Tardos 符号の結託耐性について評価と解析を行った．解析の結果, x ビット反転した場合の結託者の相関値の確率密度関数の理論値, 雑音と結託者の相関値の関係式を導出した．また, 雑音によって生じるビット反転のため, 正規ユーザの一部が大きな相関値をとり, 設定値以上の誤検出が起こることがわかった. 実験結果では, 誤検出回数と雑音によるビット反転数の関係は $f_p = \sqrt{2}x$ 程度であり, 線形的に増加する．この結果より, 雑音のある実環境において, 従来の正規分布を用いた閾値の設定方法では不十分であり, 雑音に応じた新たな閾値の設定方法を定めることが必要となることが明らかになった.

参考文献

[1] D. Boneh and J. Shaw, “Collusion-secure fingerprinting for digital data,” *IEEE Trans. Inform. Theory*, vol.44, pp.1897–1905, 1998.

[2] G. Tardos, “Optimal probabilistic fingerprint codes,” *Proc. STOC 2003*, pp.116–225, 2003.

[3] B. Škorić, S. Katzenbeisser, and M. Celik, “Symmetric Tardos fingerprinting codes for arbitrary alphabet sizes,” *Designs, Codes and Cryptography*, vol.46, no.2, pp.137–166, 2008.

[4] T. Furon, A. Guyader, and F. Cerou, “On the design and optimization of Tardos probabilistic fingerprinting codes,” *IH2008*, LNCS, vol.5284 pp. 341–356, 2008.

[5] K. Nuida, S. Fujitsu, M. Hagiwara, T, Kitagawa, H. Watanabe, K, Ogawa, and H. Imai, “An improvement of discrete Tardos fingerprinting codes,” *Des. Codes Cryptogr.*, vol.52, no.3, pp. 339–362, 2009.

[6] 明石, 栗林, 森井, “Tardos 符号のトレーサビリティの評価,” *SCIS2008*, 1D1-5, 2008.