あみだくじを用いた対話的なブラウザ履歴漏洩の研究

明治大学総合数理学部
笹航太（学部3年）, 清水雄太（学部3年）, 菊池浩明

研究背景

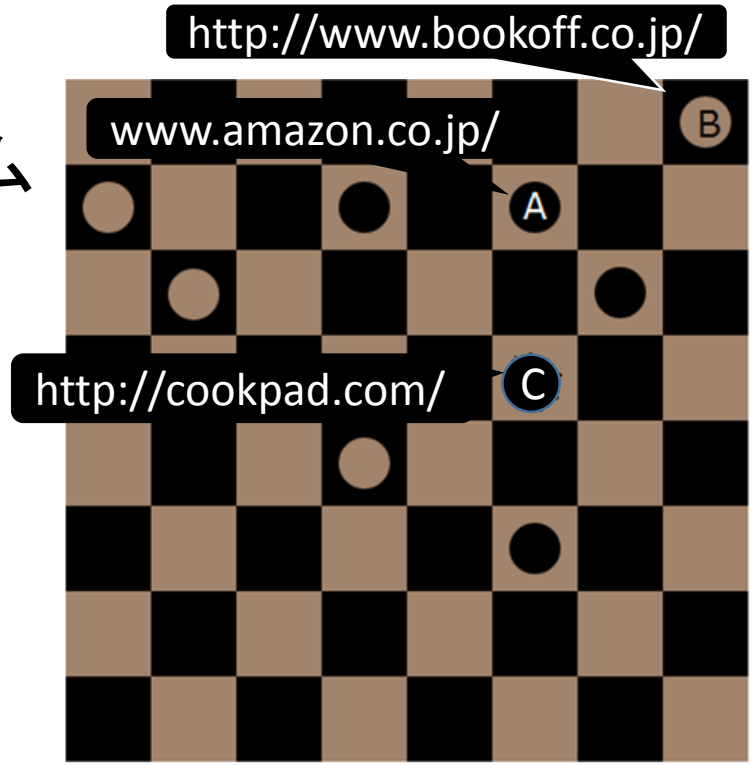
- ブラウザ履歴は重要な個人情報であると同時に、ユーザのニーズを推測することが出来る情報なので業者から狙われる可能性が高い
- 2011年, ユーザが気づかないうちに、他者にブラウザ履歴を知られてしまう, Captchaを偽装した“chessboard型盗聴攻撃”[1]が提案されている

[1] Zachary Weinberg, Eric Y. Chen, Pavithra R.Jayaraman and Collin Jackson, “I Still Know What You Visited Last Summer”,2011 IEEE Symposium on Security and Privacy, pp. 147-161, 2011.

先行研究「ウェブサイト履歴盗聴」[Weinberg 2011]

- Captchaを偽装したchessboard型履歴盗聴システム
  - Captchaとは応答者がコンピュータでないことを確認するために使われる認証システム

- chessboard型履歴盗聴システム
- A : アマゾン
- B : ブックオフ
- C : クックパッド

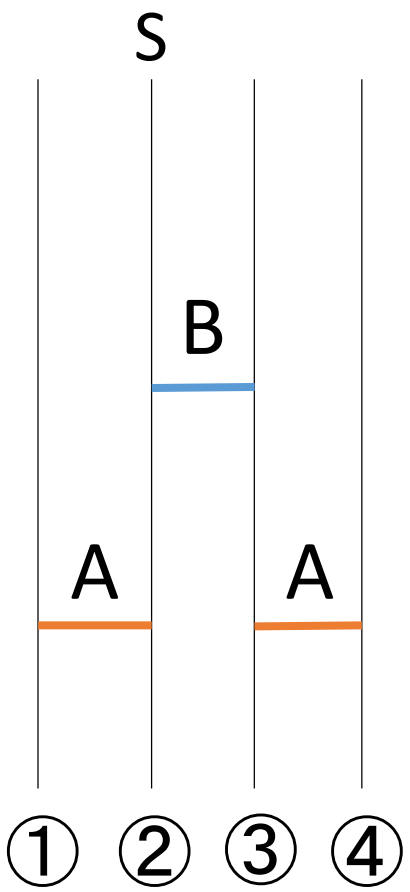


Captchaの例

chessboard型履歴盗聴システムの問題点

- 欠点
  - 1クリック1履歴しか取得できない
  - URLが多いと不自然になる
- 本研究では, 新しい攻撃を提案し, そのリスクを正しく評価する

提案方法　あみだくじを利用した履歴盗聴

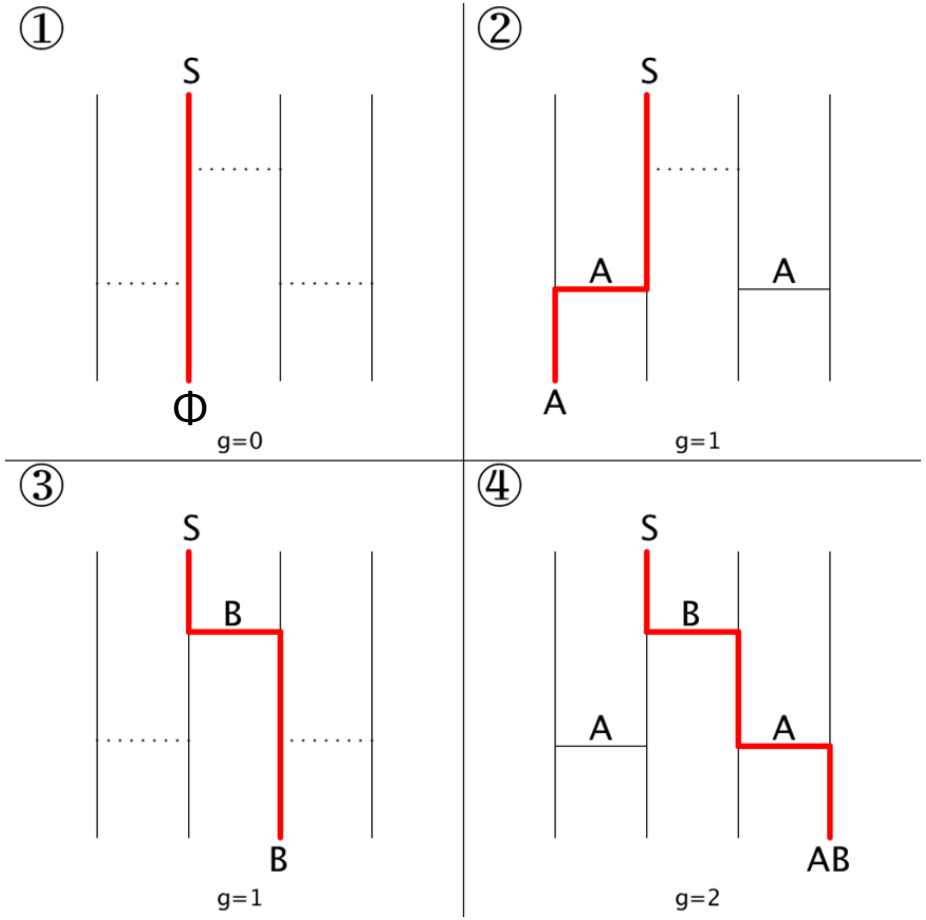


n=4

n=8

- アイデア
  - 横線にURLを割り当てることに依り, ワンクリックで複数履歴取得
  - 縦線数nを増やすことで, 取得履歴数を増やすことができる
- 問題点
  - 縦線数 n が増えると, 処理時間が増加する?
  - nが変化しなくても, 複雑度が増すことで, 処理時間が増加する?

あみだの複雑度



- あみだの複雑度をgで表す
  - gは1クリックで取得できる履歴数
  - gが増加するほど複雑である
- gが増加するほど，処理時間が増加するのでは?

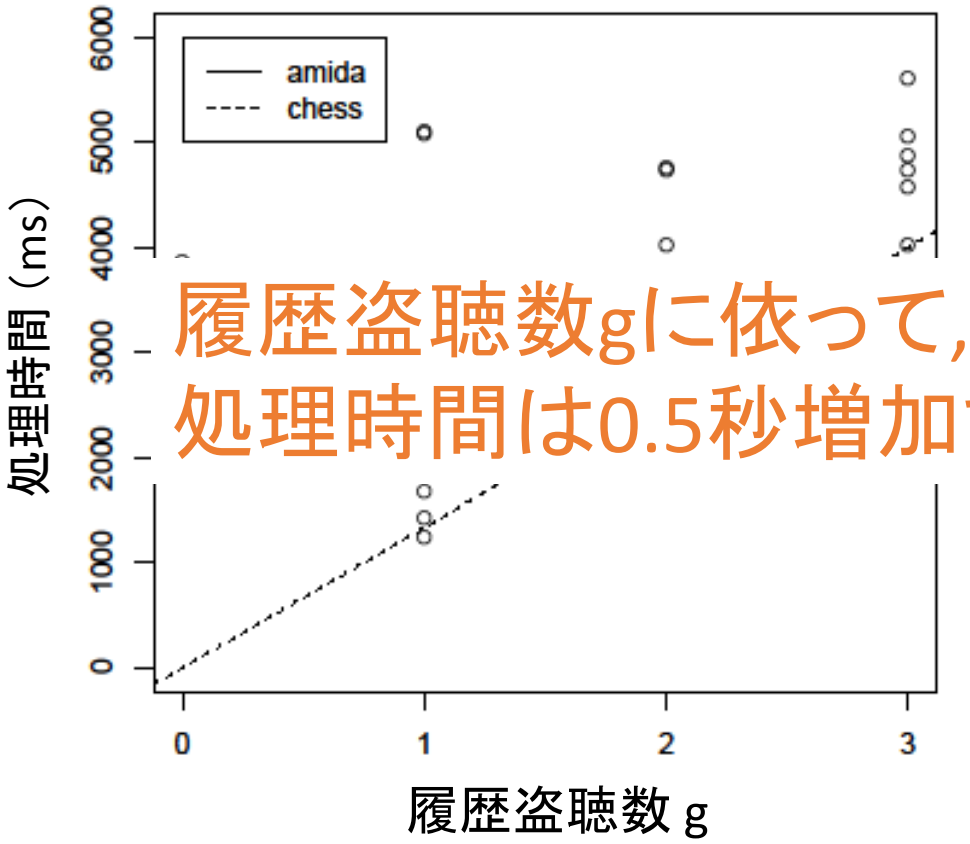
実験方法　目的

- 実験1　nとgにおける, あみだの処理時間
  - Processingを用いてランダムなあみだくじを表示する. gを最大2または3とする 提案方式で, それぞれのあみだくじを解きゴールをクリックするまでの応答時間を計測する
  - 2015年10月, 20名の被験者にランダムに20～30個のあみだくじを与えて, 処理時間を計測した
    - n=4, 8
    - g=0, 1, 2, 3
- 実験2　chessboard方式とあみだくじ方式の比較
  - 8×8マスのチェス盤にランダムに灰色と黒の駒を各5個ずつ, 計10個表示して, そのすべてをクリックするのにかかる時間を計測する
    - n=8
    - g=0, 1, 2, 3

実験1結果：nとgにおける，あみだの処理時間

	n=4	n=8
1クリックの平均時間		7
標準偏差		1.6
1履歴あたり	2.8/2=1.4秒	3.3/3=1.1秒

縦線数nに依って，
処理時間は増加するが，
履歴あたりの時間は減少する



履歴盗聴数gに依って，
処理時間は0.5秒増加する

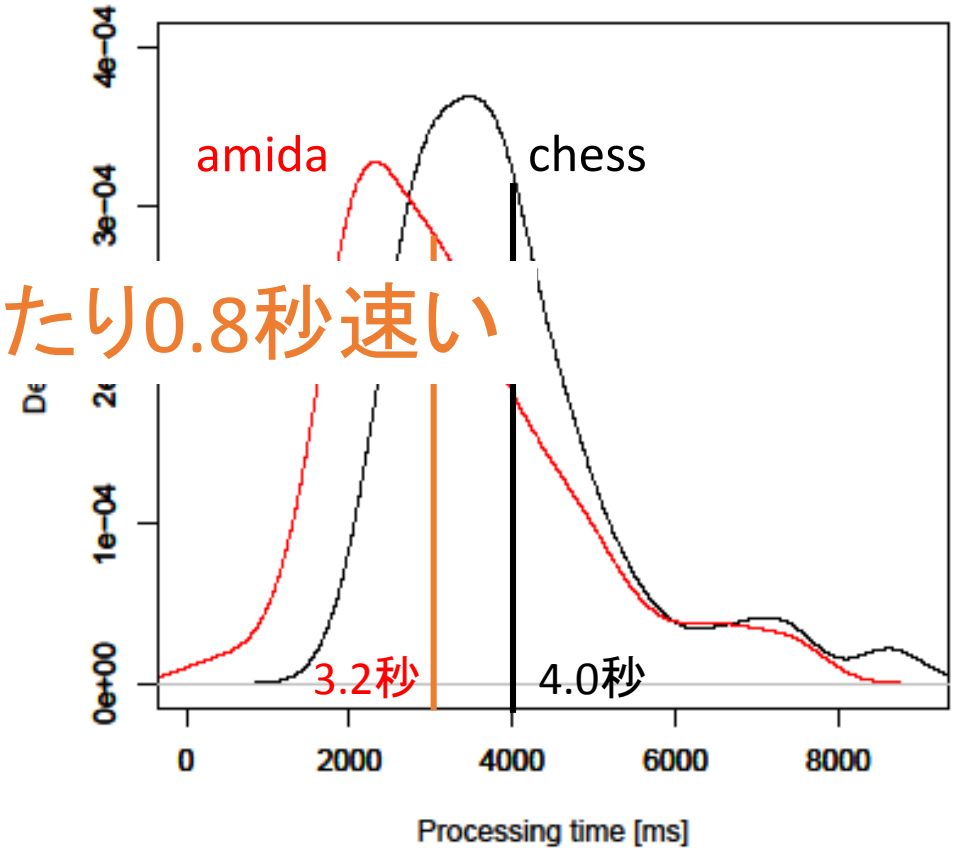
実験2結果：chessboardとあみだの比較

- n=8のあみだを利用

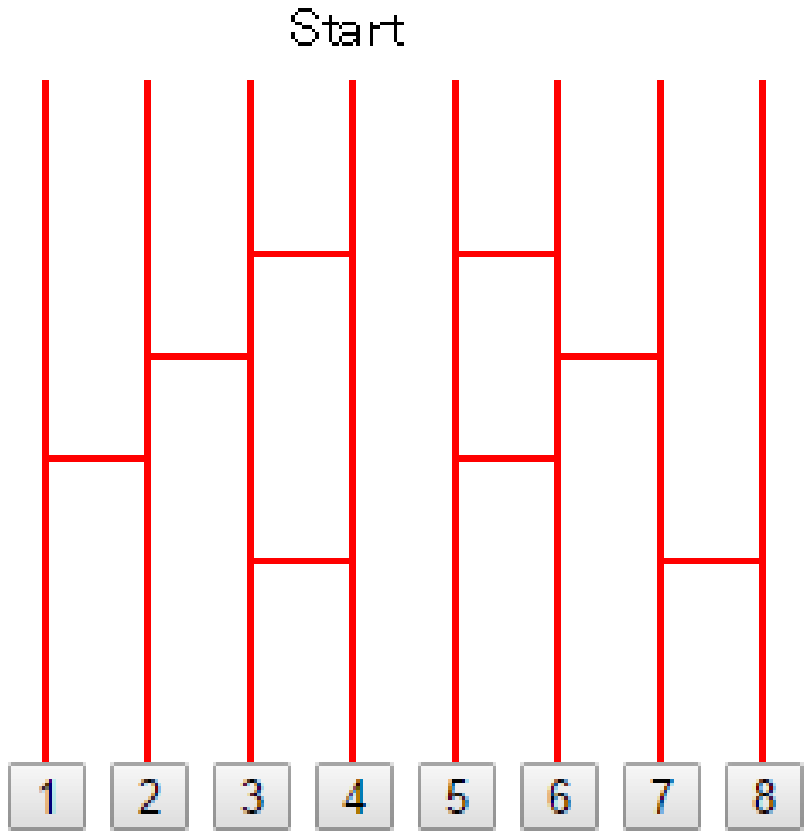
方式	chessboard	あみだくじ
g		
1クリックの平均応答時間[ms]	1334.3	3273.7
標準偏差	503.87	1449.6

あみだの方が3履歴あたり0.8秒速い

3履歴あたりの応答時間分布



http://windy.mind.meiji.ac.jp/~ksa/amida/amida8.html



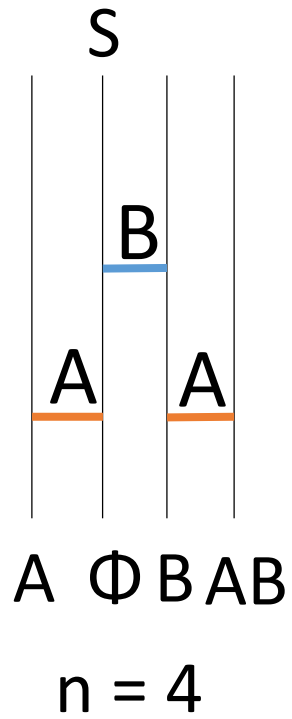
まとめ

- chessboardの1クリック１履歴しか取得できないという欠点を改善したあみだくじ方式を提案し、評価した
- 提案方式のあみだは従来方式のchessboardよりも３履歴あたり0.8秒早いことが分かった
- 今後の課題
  - 縦線の本数nを増やした場合の履歴取得の効率
  - あみだくじを知らない外国人の評価

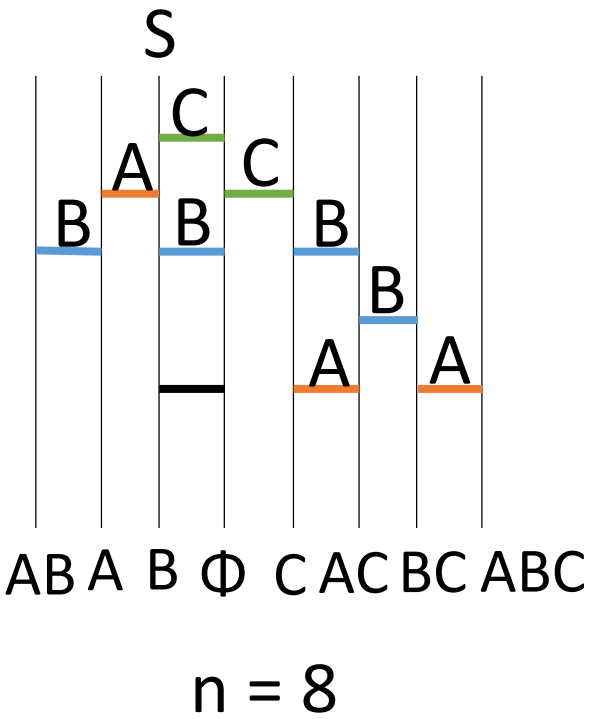
取得履歴数を増やす

縦線の数を n とすると

$n = 2^{履歴数}$



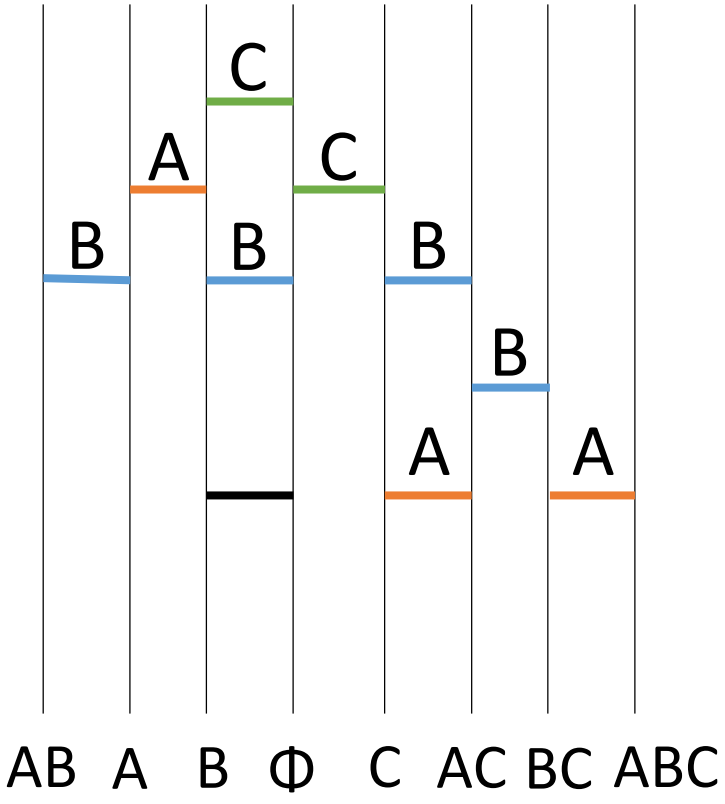
n = 4

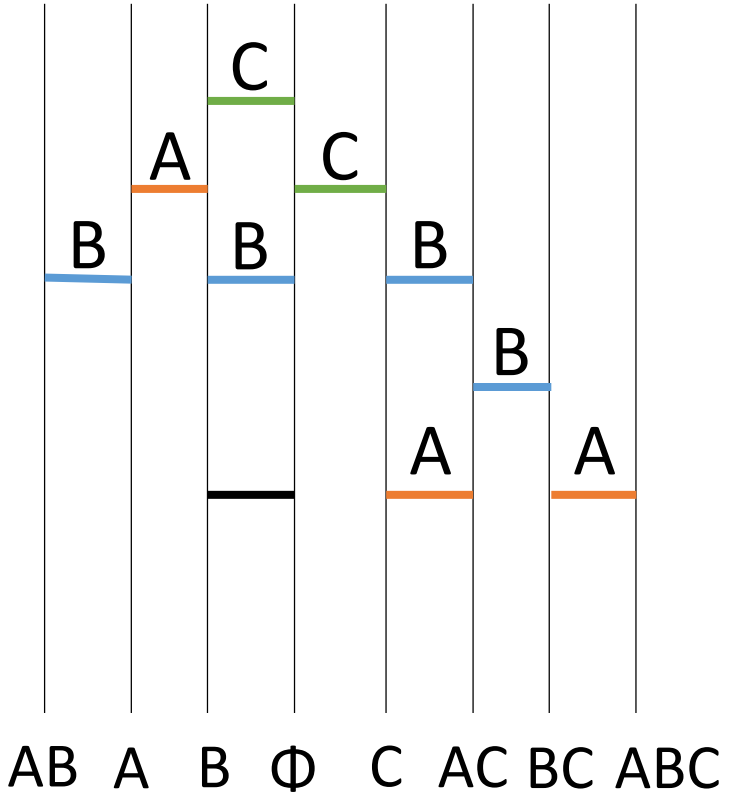


n = 8

となり n は指数関数的に増えてしまうが、
理論上は無限に履歴数を増やすことが出来る

複数本のあみだくじ作成パターン





複数本のあみだくじ作成パターン