2008 年度 プロジェクト研究

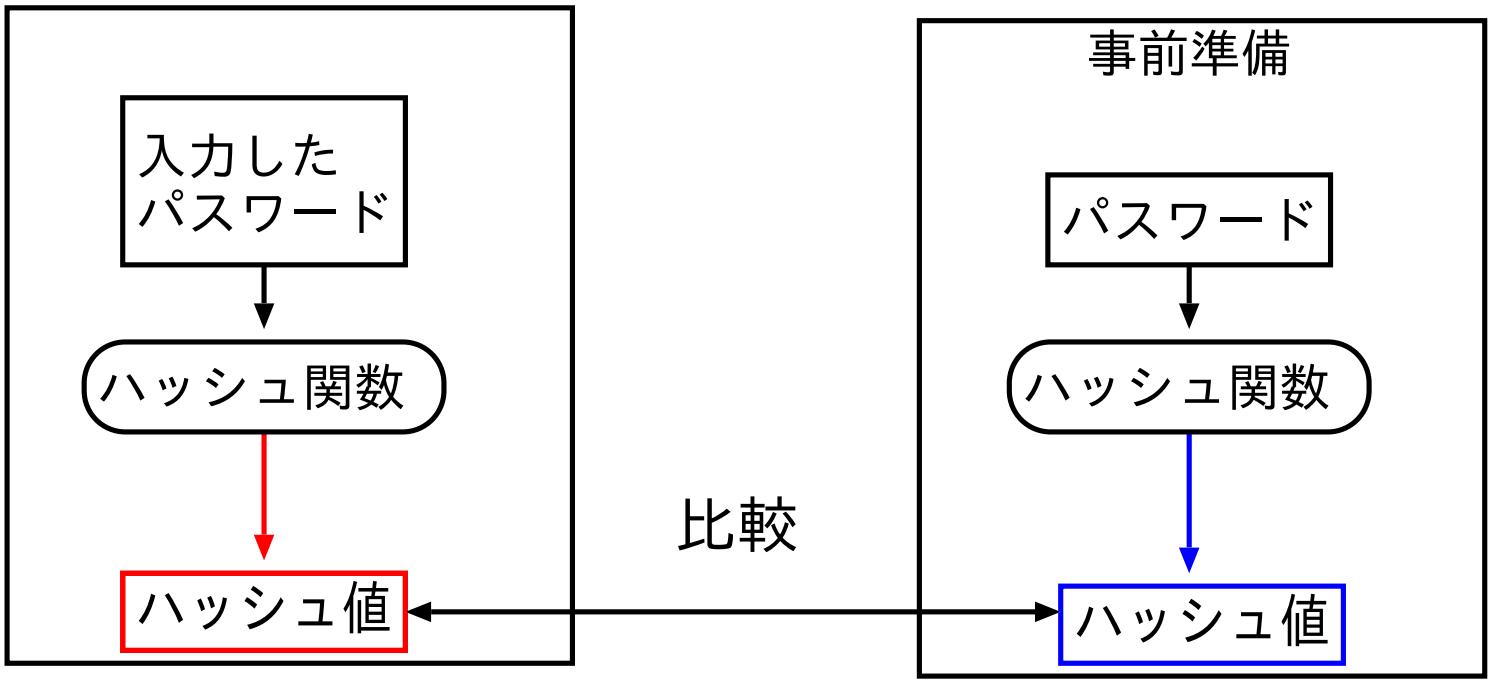
パスワード認証に用いるハッシュ関数の比較

2009 年 2 月 16 日

1090324 越智 敦司
高知工科大学 情報システム工学科
福本研究室

背景

- パスワードを用いた認証
  - ハッシュ関数が使われる



比較結果が同一であれば正当

ハッシュ関数

- 任意の長さのビット列から固定長の出力値を生成
- ハッシュ関数への要求
  - 計算が容易
    - 認証を速く行うため
  - 出力値の偏りがない
    - 第三者から元の情報が推測される可能性

↓

- パスワード認証の観点でハッシュ関数を比較
  - **MD4，MD5，SHA1，RIPEMD160**

生成時間の比較

- ハッシュ値の生成を繰り返し行いその生成時間を測る
  - 入力:**“abcdefgh”**
  - 繰り返し回数:**10,000,000** 回
  - **1** 回当たりの生成時間を平均値から算出

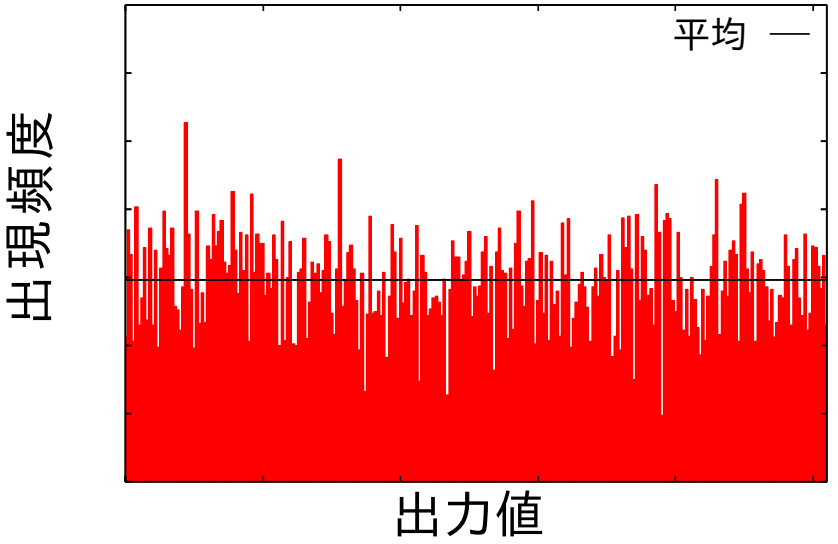
生成時間の比較結果

- 生成時間は **MD4**，**SHA1**，**MD5**，**RIPEMD160** の順に速い
  - **RIPEMD160** で **6.7μsec**，生成時間は速い

ハッシュ関数	時間 (μsec)
MD4	1.6
MD5	1.9
SHA1	1.7
RIPEMD160	6.7

出力の偏りの比較

- 入力
  - 小文字のアルファベット “a”から “z”の組合せ
  - 文字数 1 文字から 4 文字
- 出力を分類
  - 8 ビット 256 種類に分類し出現頻度を求める
  - 最も偏りの大きい値の出現確率



出力の偏りの比較結果

- **RIPEMD160** は文字数が増える毎に出現確率は減少
- その他のハッシュ関数は文字数毎に出現確率が増減
- 文字数 **2** 文字以上では各ハッシュ関数の出現確率の差が小さくなる

ハッシュ関数	**1** 文字	**2** 文字	**3** 文字	**4** 文字
MD4	0.007051	0.004709	0.003750	0.003877
MD5	0.000962	0.004524	0.003796	0.003878
SHA1	0.001265	0.003397	0.004008	0.003932
RIPEMD160	0.006832	0.004516	0.004034	0.003941

まとめ

- ハッシュ関数を生成時間と出力値の偏りについて比較
  - どのハッシュ関数もハッシュ値の生成時間は速い
  - 偏りの確率に差は大きく出なかった
- 今後の課題
  - 他のハッシュ関数での比較
  - 入力の組合せ文字列の長さを変えた場合の比較
  - 分類する数を変えての比較