覗かれても安全なパスワードについて

小橋川弓加　(指導教員：萩田真理子)

1　はじめに

パスワードとは特定の機能を使用する際に認証を得るために入力する文字や数字の羅列のことである。そのうち数字だけの列となっているものを暗証番号といい、一般的に金融機関のキャッシュカードやクレジットカード等の本人確認として使用されている。

金融機関におけるパスワードの特徴としてまず、4桁の数字で構成されていることが多いことが上げられる。「0000」から「9999」の10000パターンしか存在しないため総当たり攻撃で正しいパスワードを発見することができるという欠点がある。しかしこれに関しては入力回数に制限（通常3回まで）をつけていることで攻撃を防ぐことができている。

2つ目の特徴として、固定の番号であることが上げられる。盗み見られてしまうと他人でも使用できてしまうことが欠点である。

本研究では、パスワードを固定にするのではなく、ランダムに表示される数字をある規則性に従って暗号化して入力するシステムを作り、第三者に覗かれても破られることのないパスワードとすることが目標である。

2　構造

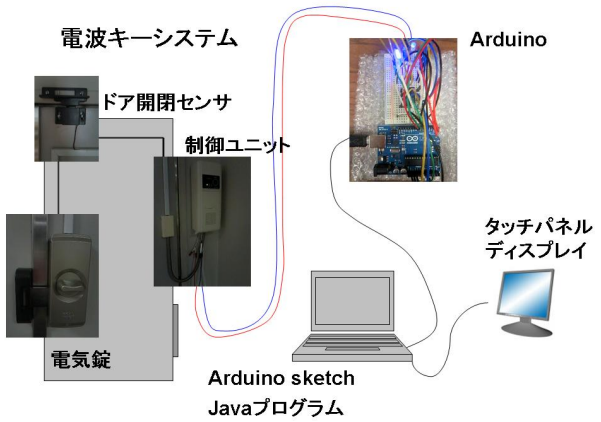

図 1: パスワードシステムの構造

図1のように主に電波キーシステムとArduino、各プログラムとタッチパネルディスプレイで構成されている。電波キーシステムはドアに設置されており、ドア開閉センサでドアの状態を認識し制御ユニットにおいて電圧を変化させることで電子錠の開錠や施錠を行っている。Arduino sketch、制御用Javaプログラムで Arduinoと制御ユニット間の電圧変化の受信や送信をし、パスワード用Javaプログラムでタッチパネルディスプレイに画面を表示している。

3　暗号化

暗号化とは元のデータを何らかの規則に従って変換し、そのままでは第三者にとって何を意味しているのかわからないデータに変換することを指す。

本研究では、表示されるランダムな数字を見てその人自身が暗号化し入力したものを、システムが復号したものと照らし合わせて判定するという方法をとる。

4　パスワード入力方法1「数字ではなく場所を覚える」

4.1　指定方法

マス目全てに0〜9の数字をランダムに挿入したものを表示し、4桁のパスワードの規則をつくる。4箇所選び、その場所の数字をそのまま入力するという条件でパスワードをつくることにする。例として図2(左)のように大きさが5×5のマス目から4箇所選び、「① ② ③ ④」の順で数字を入力することにする。

図2(右)の場合、パスワードは「3471」となる。

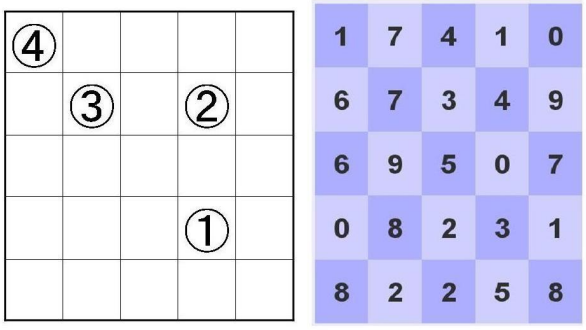

図 2: (左) パスワードを入れる位置、(右) 実際の画面

4.2　パスワードの種類

見易さ、覚えやすさの点からマス目の大きさは5×5と5×6で比較を行う。

- パスワードA　[5×5]
  ランダム (出る数字の個数に偏りがあってもよい)
- パスワードB　[5×5]
  ほぼ等確率 (1つの数字が2回または3回ずつ出る)
- パスワードC　[5×6]
  等確率 (1つの数字が3回ずつ出る)

4.3　比較

パスワードを、ランダムに押して当たる確率、何の情報もなく当てる確率、見てパスワードの入れ方がわかる確率から比較をする。

	ランダムに押して当たる確率	何の情報もなく当てる確率 (多い数字を押す)	見てパスワードの入れ方がわかる確率
パスワードA	$\left(\frac{1}{10}\right)^4$	一番多い数 i が k 回のとき $\left(\frac{k}{25}\right)^4$ 最悪の場合　1	「$abcd$」のとき $\frac{1}{a\text{の個数}} \times \frac{1}{b\text{の個数}} \times \frac{1}{c\text{の個数}} \times \frac{1}{d\text{の個数}}$ (平均0.018) 最悪の場合　1
パスワードB	$\left(\frac{1}{10}\right)^4$	$\left(\frac{2}{25}\right)^k \times \left(\frac{3}{25}\right)^{4-k}$ 最悪の場合 $\left(\frac{3}{25}\right)^4$	$\left(\frac{1}{2}\right)^k \times \left(\frac{1}{3}\right)^{4-k}$　(平均0.025) 最悪の場合　$\left(\frac{1}{2}\right)^4$
パスワードC	$\left(\frac{1}{10}\right)^4$	$\left(\frac{3}{30}\right)^4$	$\left(\frac{1}{3}\right)^4$

表 1: 3つのパスワードの比較

表 1 からランダムに押して当たる確率はどれも $\left(\frac{1}{10}\right)^4$ と等しいことから残りの 2 点について比較を行う。
パスワード A とパスワード B を比べると、平均するとパスワード A の方が良いように見えるが最悪の場合パスワード B の方が良いことがわかる。またパスワード B とパスワード C を比べると、パスワード C の方が良いことがわかる。これはパスワード B だと 1 つの数字が 2 回ずつまたは 3 回ずつ出るため、最悪の場合において何の情報もなく当てる確率では全て 3 回ずつ出る数字の時、見てパスワードの入れ方がわかる確率では全て 2 回ずつ出る数字の時、と悪い方の値をとられてしまうためである。
これらよりマス目の大きさが 5×6 で数字が等確率となる表示方法を採用する。

5 パスワード入力方法 2「暗号化の計算を入力者が行う」

本研究では、パスワード入力方法 1 の安全性を更に高めるために、入力する人が大変になり過ぎない程度の暗号化の計算を入力者の頭の中で行うようにすることで改良し、評価した。

5.1 パスワードとする数字の条件

パスワードとする数字の選び方として

- そのまま数字を入力する方法
- 演算をした結果を入力する方法

の 2 種類がある。演算をした結果を入力する方法の条件は

$$k_0a_0 + k_1a_1 + k_2a_2 + \ldots + k_ha_h + x \pmod{10}$$

a_p は表示されているものから選んだ数字であり、$k_q = 1, 3, 7, 9$、h は 0 以上で (表示されている数字の数 -1) 以下の整数、x は 0 以上の整数である。
ここで暗号化の計算において $a_r \cdot a_s \pmod{10}$ は使用できない。偶数 · 偶数 = 偶数、偶数 · 奇数 = 偶数、奇数 · 奇数 = 奇数 となることから乗算を行うと偶数の確率が高くなるためである。
今回マス目の大きさは 5×6 とするため $\max h = 29$ となり、パスワードとなる数字の選び方は 10^{30} 通り存在し、十分多い数から選ぶことができる。計算のし易さの点から $\max h = 2$、$k_i = 0$ または 1 で実装した。

この条件で以下のパスワードを作成した。全ての計算について $\pmod{10}$ を適用するものとする。

- パスワード D :「$a_0 + a_1\ b\ c\ d$」
- パスワード E :「$a_0 + a_1\ b_0 + b_1\ c\ d$」
- パスワード F :「$a_0 + a_1 + a_2\ b\ c\ d$」

5.2 安全性の評価

まず、見てパスワードの入れ方がわかる確率で評価を行う。桁ごとの入力方法別に場合の数を求めると

- a(数字をそのまま入力する場合) :3 通り
- $(a_0 + a_1)$: $\begin{cases} 45 \text{ 通り} & \text{(奇数の場合)} \\ 42 \text{ 通り} & \text{(偶数の場合)} \end{cases}$
- $(a_0 + a_1 + a_2)$:406 通り

これらよりパスワードごとの確率は表 2 のようになる。

パスワード C	パスワード D	パスワード E	パスワード F
$(\frac{1}{3})^4$	$\frac{1}{42} \cdot (\frac{1}{3})^3 = \frac{1}{1134} > (\frac{1}{10})^4$	$(\frac{1}{42} \cdot \frac{1}{3})^2 = (\frac{1}{126})^2 < (\frac{1}{10})^4$	$\frac{1}{406} \cdot (\frac{1}{3})^3 = \frac{1}{10962} < (\frac{1}{10})^4$

表 2: 見てパスワードの入れ方がわかる確率での比較

表 2 より確率が $(\frac{1}{10})^4$ 以下となるパスワード E とパスワード F は安全性が高いと言える。
また、見てランダムに入力して当たる確率は

- パスワード D、パスワード F: $\frac{1}{10} \cdot (\frac{1}{3})^3$
- パスワード E: $(\frac{1}{10})^2 \cdot (\frac{1}{3})^2$

となることからパスワード E が最も安全性が高い。
よって演算を行う桁が多い程安全性が高いことがわかる。

6 通常の鍵と本システムの比較

通常の鍵を使用する場合と本システムを利用する場合で開錠にかかる時間 (施錠されていることを確認し開錠してドアを開けるまでの時間) の比較を行った。

	パスワード C	パスワード E	パスワード F	通常の鍵
最短	5”93	7”11	7”34	8”50
最長	11”22	11”19	15”43	32”60
平均	7”31	8”85	10”49	16”75

表 3: 開錠にかかる時間の比較

表 3 より通常の鍵より本パスワードシステムを利用する方が短時間で開錠できるという結果になった。また暗号化の計算を行うよりもそのまま入力する方が短時間にはなるが、安全性を考慮するとパスワード E が最適である。

7 まとめ

表示する数字の個数については 0 から 9 の数字を等確率で出す場合に最も良い結果が得られるため、10 の倍数個が最適である。また、マス目の大きさが 5×6 の表示で演算を行うパスワードについては 1 つの桁についての演算の難易度に関わらず、演算を行う桁数が多い程安全性が高くなる。パスワード E ならランダムに押して当たる確率、何の情報もなく当てる確率、見てパスワードの入れ方がわかる確率が $(\frac{1}{10})^4$ 以下となる安全性の高いパスワードであり開錠にかかる時間も短く実装に耐え得るパスワードと言える。

謝辞

本研究を進めるにあたって、ご助言、ご指導いただきました冨樫雅文先生、浅本紀子先生に深く感謝いたします。