Optimal ec-PIN Guessing

MARKUS G. KUHN

**Known:** 12 offset digits from magnetic stripe:

Offset 1: \( O_1 = (O_{1,1}, O_{1,2}, O_{1,3}, O_{1,4}) \)

Offset 2: \( O_2 = (O_{2,1}, O_{2,2}, O_{2,3}, O_{2,4}) \)

Offset 3: \( O_3 = (O_{3,1}, O_{3,2}, O_{3,3}, O_{3,4}) \)

**Wanted:** four most likely PIN digits

\[ \hat{P} = (\hat{P}_1, \hat{P}_2, \hat{P}_3, \hat{P}_4) \]

**Define:**

\[ \tilde{P}_j = \text{random variable for } j\text{-th digit in PIN} \]

\[ \tilde{O}_{i,j} = \text{random variable for } j\text{-th digit in offset } i \]

for all \( 1 \leq i \leq 3 \) and \( 1 \leq j \leq 4 \).

**Distributions:**

\[
p(\tilde{P}_j = k) = \begin{cases} 
0/16, & \text{if } j = 1 \text{ and } k = 0 \\
4/16, & \text{if } j = 1 \text{ and } k = 1 \\
2/16, & \text{if } j > 1 \text{ and } k \in \{0, 1\} \\
2/16, & \text{if } k \in \{2, \ldots, 5\} \\
1/16, & \text{if } k \in \{6, \ldots, 9\}
\end{cases}
\]

\[
p(\tilde{O}_{i,j} = k | \tilde{P}_j = l) = \begin{cases} 
2/16, & \text{if } (l - k) \text{ mod } 10 \in \{0, \ldots, 5\} \\
1/16, & \text{if } (l - k) \text{ mod } 10 \in \{6, \ldots, 9\}
\end{cases}
\]
A most likely PIN $\hat{P}$ is a $P$ for which
\[ p(\hat{P} = P | \forall i : \tilde{O}_i = O_i ) \]
is maximal. PIN digits are independent, therefore we look at per-digit probability
\[ p(\tilde{P}_j = P_j | \forall i : \tilde{O}_{i,j} = O_{i,j} ) \]
and get best PIN as the combination of most likely digits.

We turn around this conditional probability (Bayes’ theorem)
\[ p(\tilde{P}_j = P_j | \forall i : \tilde{O}_{i,j} = O_{i,j} ) \]
\[ = \frac{ p(\tilde{P}_j = P_j \land \forall i : \tilde{O}_{i,j} = O_{i,j} ) }{ p(\forall i : \tilde{O}_{i,j} = O_{i,j} ) } \]
\[ = \frac{ p(\forall i : \tilde{O}_{i,j} = O_{i,j} | \tilde{P}_j = P_j ) \cdot p(\tilde{P}_j = P_j ) }{ p(\forall i : \tilde{O}_{i,j} = O_{i,j} ) } \]
\[ = \frac{ p(\forall i : \tilde{O}_{i,j} = O_{i,j} | \tilde{P}_j = P_j ) \cdot p(\tilde{P}_j = P_j ) }{ \sum_{k=0}^{9} p(\forall i : \tilde{O}_{i,j} = O_{i,j} | \tilde{P}_j = k ) \cdot p(\tilde{P}_j = k ) } \]
and since all three offsets are independent
\[ = \frac{ \prod_{i=1}^{3} p(\tilde{O}_{i,j} = O_{i,j} | \tilde{P}_j = P_j ) \cdot p(\tilde{P}_j = P_j ) }{ \sum_{k=0}^{9} \prod_{i=1}^{3} p(\tilde{O}_{i,j} = O_{i,j} | \tilde{P}_j = k ) \cdot p(\tilde{P}_j = k ) } \]

Now calculate this for all $P_j \in \{0, \ldots, 9\}$ and determine the $\hat{P}_j$ with maximum probability.
What success rate do we expect with a randomly picked card?

For PIN digit $j$: Try all $16^4$ combinations of hexadecimal digits $(W, X, Y, Z)$. Like the bank, determine the PIN and offsets:

$$P_j := \begin{cases} W \mod 10, & \text{if } W \mod 10 > 0 \text{ or } j > 1 \\ 1, & \text{if } W \mod 10 = 0 \text{ and } j = 1 \end{cases}$$

$$O_{1,j} := (P_j - X) \mod 10$$

$$O_{2,j} := (P_j - Y) \mod 10$$

$$O_{3,j} := (P_j - Z) \mod 10$$

We have now $16^4$ simulated cards with realistic PIN and offset digit distribution.

Now, determine most likely PIN digit $\hat{P}_j$ for all of those $16^4$ cards and compare $\hat{P}_j$ with $P_j$. The measured success rates are:

- digit 1: $0.27856 \approx 28\% \approx 1/3.6$
- digit 2: $0.20312 \approx 20\% \approx 1/4.9$
- digit 3: $0.20312 \approx 20\% \approx 1/4.9$
- digit 4: $0.20312 \approx 20\% \approx 1/4.9$

Note: With a good PIN-generation algorithm, we would have expected 1/9 for first digit and 1/10 for remaining three.

Single attempt success rate for all four digits:

$$0.27856 \cdot 0.20312^3 \approx 0.0023346 \approx 0.233\% \approx 1/428$$
A card thief has at least three attempts to enter a PIN and most second or third-best PINs have a similar success probability, therefore

$$3 \cdot 0.0023346 \approx 0.7\% \approx 1/150$$

This is an expected value for a randomly selected card. Some individual cards with offsets like 0000/6666/6555 allow success rates as high as 1.896\% \approx 1/52.7 in three attempts.

Comparison: With a good PIN algorithm, we would have expected

$$3 \cdot 1/9 \cdot 1/10 \cdot 1/10 \cdot 1/10 = 1/3000 \approx 0.033\%.$$ 

In other words, the security of the 4-digit ec-PIN system is worse than that of a good 3-digit system (with 1/300 \approx 0.33\% success rate).
PIN Calculation for EuroCheque ATM Debit Cards

Data on magnetic stripe track 3 (ISO 4909):
- Bank routing number: 24358270
- Account number: 0012136399
- Card sequence number: 1

16 decimal digits in BCD = 64 bits

- PIN used by customer:
  - first digit: \(0 \rightarrow 1\)

- Institute-Key: (56 bits)
- Pool-Key-1: (56 bits)
- Pool-Key-3 / Offset-3 with Pool-Key-2 / Offset-2

DES Encryption

- DES Encryption
- Pool-Key-1
- Offset-1 on track 3:

Data on magnetic stripe track 3 (ISO 4909):
- Bank routing number: 24358270
- Account number: 0012136399
- Card sequence number: 1

16 decimal digits in BCD = 64 bits

- PIN used by customer:
  - first digit: \(0 \rightarrow 1\)

- Institute-Key: (56 bits)
- Pool-Key-1: (56 bits)
- Pool-Key-3 / Offset-3 with Pool-Key-2 / Offset-2

DES Encryption

- DES Encryption
- Pool-Key-1
- Offset-1 on track 3:

Data on magnetic stripe track 3 (ISO 4909):
- Bank routing number: 24358270
- Account number: 0012136399
- Card sequence number: 1

16 decimal digits in BCD = 64 bits

- PIN used by customer:
  - first digit: \(0 \rightarrow 1\)

- Institute-Key: (56 bits)
- Pool-Key-1: (56 bits)
- Pool-Key-3 / Offset-3 with Pool-Key-2 / Offset-2

DES Encryption

- DES Encryption
- Pool-Key-1
- Offset-1 on track 3:

Data on magnetic stripe track 3 (ISO 4909):
- Bank routing number: 24358270
- Account number: 0012136399
- Card sequence number: 1

16 decimal digits in BCD = 64 bits

- PIN used by customer:
  - first digit: \(0 \rightarrow 1\)

- Institute-Key: (56 bits)
- Pool-Key-1: (56 bits)
- Pool-Key-3 / Offset-3 with Pool-Key-2 / Offset-2

DES Encryption

- DES Encryption
- Pool-Key-1
- Offset-1 on track 3:

Data on magnetic stripe track 3 (ISO 4909):
- Bank routing number: 24358270
- Account number: 0012136399
- Card sequence number: 1

16 decimal digits in BCD = 64 bits

- PIN used by customer:
  - first digit: \(0 \rightarrow 1\)

- Institute-Key: (56 bits)
- Pool-Key-1: (56 bits)
- Pool-Key-3 / Offset-3 with Pool-Key-2 / Offset-2

DES Encryption

- DES Encryption
- Pool-Key-1
- Offset-1 on track 3:

Data on magnetic stripe track 3 (ISO 4909):
- Bank routing number: 24358270
- Account number: 0012136399
- Card sequence number: 1

16 decimal digits in BCD = 64 bits

- PIN used by customer:
  - first digit: \(0 \rightarrow 1\)

- Institute-Key: (56 bits)
- Pool-Key-1: (56 bits)
- Pool-Key-3 / Offset-3 with Pool-Key-2 / Offset-2

DES Encryption

- DES Encryption
- Pool-Key-1
- Offset-1 on track 3:

Data on magnetic stripe track 3 (ISO 4909):
- Bank routing number: 24358270
- Account number: 0012136399
- Card sequence number: 1

16 decimal digits in BCD = 64 bits

- PIN used by customer:
  - first digit: \(0 \rightarrow 1\)

- Institute-Key: (56 bits)
- Pool-Key-1: (56 bits)
- Pool-Key-3 / Offset-3 with Pool-Key-2 / Offset-2

DES Encryption

- DES Encryption
- Pool-Key-1
- Offset-1 on track 3:

Data on magnetic stripe track 3 (ISO 4909):
- Bank routing number: 24358270
- Account number: 0012136399
- Card sequence number: 1

16 decimal digits in BCD = 64 bits

- PIN used by customer:
  - first digit: \(0 \rightarrow 1\)

- Institute-Key: (56 bits)
- Pool-Key-1: (56 bits)
- Pool-Key-3 / Offset-3 with Pool-Key-2 / Offset-2

DES Encryption

- DES Encryption
- Pool-Key-1
- Offset-1 on track 3: