ATM PIN generation – a formal mathematical model to generate PIN using regular grammar, context free grammar and recognition through finite state machine, pushdown automata

S. Vaithyasubramanian*

Department of Mathematics,
Sathyabama Institute of Science and Technology,
Chennai, India
Email: discretevs@gmail.com
*Corresponding author

A. Christy

Faculty of Computing,
Sathyabama Institute of Science and Technology,
Chennai, India
Email: ac.christy@gmail.com

Abstract: A secret passcode composed of numbers in authenticating the genuine user is recognised as personal identification number (PIN). A PIN is utilised to authenticate the identity of the legitimate person to access debit/credit card in an ATM or online. In general personal identification number is used to validate the legitimate user for transactions like credit card, debit card; online and also in accessing mobile telephones. In banking sectors, as a part of two factor authentication ATM card assumes noteworthy part, PIN serves as a legalised application to distinguish the authenticated user. PIN commonly contains four digits; to generate this four digit access code new behavioural model has been proposed. This paper exhibits PIN generation technique made out of a finite number of states utilising 'regular grammar' and 'context free grammar'. Programming language Python generating PIN of four digit numbers is also offered in this paper. To perceive the produced four-digit ATM PIN computational mathematical model known as a 'finite state machine' and 'pushdown automata' has been utilised.

Keywords: automated teller machine; ATM; personal identification number; PIN; access code; mathematical model; computational model; regular grammar; context free grammar; finite state machine; pushdown automata.

Reference to this paper should be made as follows: Vaithyasubramanian, S. and Christy, A. (2019) 'ATM PIN generation – a formal mathematical model to generate PIN using regular grammar, context free grammar and recognition through finite state machine, pushdown automata', *Int. J. Internet Protocol Technology*, Vol. 12, No. 1, pp.11–15.

Biographical notes: S. Vaithyasubramanian started his teaching carrier in the year 2002. Since 2007, he is associated with Department of Mathematics, Sathyabama University. His interested areas of research are formal languages, Petri net, mathematical modelling, information security and CAPTCHAs. He has published various articles in his fields of research in reputed journals.

A. Christy is a Professor of Computer Science at Sathyabama Institute of Science and Technology, Chennai. Her interested areas of research are text mining, data mining, information retrieval, databases and natural language processing. She has published various articles in his fields of research in reputed journals.

1 Introduction

Automated teller machines (ATM) have almost replaced the banks for many frequently used customer operations as cash withdrawals, deposits, statement generations, fund transfers, cheque requests, etc. for its ease of operation, closest accessibility, paperless job and instant economy benefits. An ATM is a wellbeing basic and constant framework that is exceedingly intricate in outline and execution. Being highly customer-oriented, the two keys to any ATM transactions are the bank card and the PIN (https://banking.about.com/od/securityandsafety/p/pin number.htm; https://banking.about.com/od/checkingaccounts/g/pinnumber2.htm2; https://homesecurity.about.com/od/online/fl/Using-PINs-Safely.htm). Unlike account numbers, PINs can be redundant across customers

yet very crucial for protection of information and money. First time ATM PINs are generated by the bank and given to respective account holder confidentially, post which customer can change his PIN any number of times. ATM PINs created for customer/account holders are generally random generated by the system tool applied for PIN generations which are ideally four-digit numbers. At present, these first time PINs are individually given to relevant person with a specification of PIN legitimacy time for user change (http://www.knowledgehub.co.in/2010/07/meaning-ofnumbers-on-debit-credit-card.html; http://www.investorwords.com/3684/personal_identification_number.html#ixzz399wdZEU6; https://www.techopedia.com/definition/12128/personal-identification-number-pin). By making the generation of first time PINs with this automated computation method, the computation process is simple, faster and cost-effective.

Managing numerous accounts/personal devices and data with set of few PINs which can be recalled is very difficult and quite challenging (https://hackedgadgets.com/2006/12/01/atm-pinnumbers-hacked/). Whether the strategy conveyed is by word technique, i.e., by converting a 'word' to corresponding numbers on keypad, date method, i.e., key dates in different configuration, saving PIN on mobile phone in unidentifiable way or using mathematical logic to mask the direct PIN, forever it is better and fine to apply a technically stronger PIN to crack (https://homesecurity.about.com/od/online/fl/Using-PINs-Safely.htm; Akomolafe and Afeni, 2014; Bond and Zielinski, 2003).

User gets the gateway using the ATM card but only with usage of PIN, access to confidential data is granted. Unlike other PINs/passwords which demands a combination of alphabets, numbers and special characters or even few which adds up upper case alphabets, ATM PINs have always been numbers. Authentication using fingerprints also implemented in addition to PIN. Study is going on in this interesting topic for modelling, effective security of ATM systems by implementing biometric, facial recognition and audio signals (Babatunde and Charles, 2013; Wu, 2011; Scarfo, 2017; Karovaliya et al., 2015; Lee et al., 2016). Analysis of various attacks on ATM PIN also discussed (Stanekova and Stanek, 2013).

Universally ATM PIN is a string of length four characters. To generate the four digits PIN number new techniques has been proposed in this paper. To design the generation of four-digit ATM PIN From the field of theoretical computer science, regular grammar and context free grammar have been used. To recognise the generated PIN, finite state automata/finite state machine and pushdown automata are used respectively.

2 History of ATM and ATM PIN

ATM – an electronic banking outlet, which enables clients to finish essential monetary transactions without the guide of a branch agent. Luther Simjian (https://inventors.about.com/od/astartinventions/a/atm_2.htm), in 1939 brought in a thought of creating a 'hole-in-the-wall machine' (https://www.walesonline.co.uk/business/personalfinance/hole-wall-machine-50-years-13242356; Irish, 1998) that would support customers in financial transactions partially as an executive. He further experimented his ATM machine after applying for 20 patents. In 1967, John Shepherd-Barron (https://www.engineersgarage.com/inventionstories/atm-history) invented and installed an ATM in Barclays Bank, London followed by Don Wetzel (https://inventors.about.com/od/astartinventions/a/atm_2.htm) in 1968 with his US made ATM. The first ATMs, which worked on radiation and low-coercive magnetism, used printed rubber bands which wound back at the end of each customer transaction.

Post 1980s, ATM has seen remarkable development in terms of market and technology. At present ATM has more or less every part of banking services starting from cash withdrawal, balance check, cash deposit, bank statement, etc. which avoids queuing at bank branches. Market for ATMs has demanded innovative strategies from the banks and technology advancements brought in touch and mobile interactive tools. Likewise with several technology development, ATM security has its own threats on users as threat on cracking of PIN, money withdrawn, card lost and personal information by swiping in, leakage of account particulars on-screen and so forth (https://hackedgadgets.com/2006/12/01/atm-pinnumbers-hacked/; Bond and Zielinski, 2003).

PINs were first used in ATMs in late 1960s and its security have caught critical attention from 1990s when users were less concerned about complexity of their PINS which led to easier hacking of quite predictable credentials. Today, institutions invest huge amount in buying third party tools to random generate their first time PINs, passwords for their clients; and users finding it complex to update and track their various business points (https://inventors.about.com/od/astartinventions/a/atm_2.htm).

The thought of an individual ID number or PIN was concocted by John Shepherd Barron (https://inventors.about.com/od/astartinventions/a/atm_2.htm), Barron's wife Caroline honed PIN system by changing John's proposed six digit number to four as it was less demanding to recall.

3 Existing methods of ATM PIN generation

- IBM 3624: most basic ATM model generated ATM pin named as natural pin using IBM method. The pin generation is by encrypting primary account number where encryption key is exclusively used. PIN numbers generated by this method are assigned to each individual account number/card by service provider. Since they are derived from primary account number user cannot select their PIN. If the card is issued again new pin must be generated (Bond and Zielinski, 2003; Akomolafe and Afeni, 2014).
- IBM 3624 + offset: in this method user is allowed to select their PIN which is interpreted with natural PIN based on its modulo value to derive the respective

offset value. The offset can be stored in the database of the issuer or on the user card track (Akomolafe and Afeni, 2014).

- VISA method: unlike the earlier IBM PIN derivation this Visa method generates PIN verification value (PVV) similar to offset value, instead of generating the PIN. PVV itself is a logical value calculated from PIN validation key index (PVKI) which gets encrypted. The PVV can be stored in the database of the issuer or on the user card track (Akomolafe and Afeni, 2014).

4 Proposed ATM PIN generation

Each business is unique and so is their security and information protection system. Regular grammar, context free grammar, finite state machine and pushdown automata would be a structured and ready to deploy tool as briefed below on its objective and framework logic.

4.1 Framework model I – regular grammar generating PIN

Generation of four-digit ATM PIN by regular expression (RE) and context free grammar is as follows: RE is the traditional notation of regular grammar. In the classification of Chomsky hierarchy of formal grammars, regular grammar is type-3. The strings generated and accepted by the grammar is expressed in a declarative way by RE. In systems like UNIX grep, Lexical-analyser RE serves as the input languages to process strings. Formally a regular grammar is four-tuple defined as G = (V, T, P, S), where S: the start symbol which belongs to V, V: a set of non-terminal variable, T: set of terminal variable, P: set of all the production rules of the forms: S → Aa/bB/a/b/ε, where S, A and B are a non-terminal in V and a, b is a terminal in T, and ε is the empty string.

Regular grammar generating PIN:

Start symbol S = A, V = {A, B, C, D}, T = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}

Production rule as follows:

A → B0/B1/B2/B3/B4/B5/B6/B7/B8/B9

B → C0/C1/C2/C3/C4/C5/C6/C7/C8/C9

C → D0/D1/D2/D3/D4/D5/D6/D7/D8/D9

D → 0/1/2/3/4/5/6/7/8/9

Regular expression:

$(0\backslash1\backslash2\backslash3\backslash4\backslash5\backslash6\backslash7\backslash8\backslash9)^{+}(0\backslash1\backslash2\backslash3\backslash4\backslash5\backslash6\backslash7\backslash8\backslash9)^{+}(0\backslash1\backslash2\backslash3\backslash4\backslash5\backslash6\backslash7\backslash8\backslash9)^{+}(0\backslash1\backslash2\backslash3\backslash4\backslash5\backslash6\backslash7\backslash8\backslash9)^{+}$

4.2 Framework model II – context free grammar generating PIN

In the classification of Chomsky hierarchy of formal grammars, context free grammar is type-2. A context free grammar is expressed well in Backus-Naur form (BNF). context free grammars are exclusively different from dependency grammar and are referred as phrase structure grammars. To create/generate pattern of strings context free grammar is used. The generation/creation of pattern of strings are by set of recursive production rules. Context free grammar is essential in linguistics to characterise the organisation of conveying a statement and expressions in common language. In computer science, context free grammars are employed for tagging the formation of programming languages and other official languages (Hopcroft and Ullman, 1979).

Formally a context free grammar is four-tuple defined as G = (V, T, P, S), where S: the start symbol belongs to V, V: a set of non-terminal variable, T: set of terminal variable, P: set of all the production rules of the forms: S → Aa/bB/a/b/ε, where S, A and B are a non-terminal in V and a, b is a terminal in T, and ε is the empty string.

Context free grammar generating PIN:

Start symbol: S

V = {A, B, C, D, S}

T: 0/1/2/3/4/5/6/7/8/9

Production rule:

S → 0BCD/1BCD/2BCD/3BCD/4BCD/5BCD/6BCD/ 7BCD/8BCD/9BCD

B → 0/1/2/3/4/5/6/7/8/9,

C → 0/1/2/3/4/5/6/7/8/9,

D → 0/1/2/3/4/5/6/7/8/9

4.3 Framework model III – PYTHON generating all possible four-digit ATM PIN

```
import random
file = open('randomnumbers-string.txt', 'a+')
n = int(input('Enter the no of samples'))
# no of random numbers to be generated
for i in range(0, n):
    a = ''
    for i in range(0, 4):
        a += str(random.randint(0, 9))
    print a
    file.write(a+'\n')
```

OUTPUT:

5455, 2481, 7238, 7904, 6637

5 Recognition of the generated PIN using FSA and PDA

A finite state automata is a behaviour model, used to design digital logic or computer programs composed of a finite number of states known as input states and output states, transition from input state to output state. The process originates from initial state also called as start state, based on the input transition takes place from one state to another state. A string will be recognised as accepted for a particular

language generated by a finite state automata only if that strings derivation starts from the initial state and ends at the final state (Hopcroft and Ullman, 1979). Finite state machines can tackle an extensive number of issues, among which are electronic outline robotisation, correspondence convention plan, parsing and other designing applications. In science and computerised reasoning examination, state machines or orders of state machines are in some cases used to illustrate neurological frameworks and in etymology to portray the linguistic uses of regular languages (https://whatis.techtarget.com/definition/finite-statemachine; https://tr.cyclopaedia.net/wiki/Finite-state_ machine).

Finite state machine recognising ATM PIN generated by RE is modelled as five tuple M = {Q, Fi, Fa, Σ, δ} where Q = set of all states, Fi = initial state, Fa = final state, Σ = set of all input alphabets, δ = transition function. Here M = {Q, Fi, Fa, Σ, δ} where Q = no. of states = $\{q_0, q_1, q_2, q_3, q_4\}$; initial state: Fi = q_0; final state: Fa= q_4; input alphabets denoted as $ = Σ = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}; transition function: $\delta: Q \times \Sigma \rightarrow Q^*$ and defined as $\delta(q_0, \$) = q_1$; $\delta(q_1, \$) = q_2$; $\delta(q_2, \$) = q_3$; $\delta(q_3, \$) = q_4$.

Figure 1 Finite state machine recognising generated ATM PIN

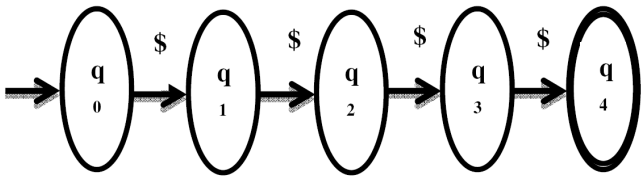


Table 1 Transition table

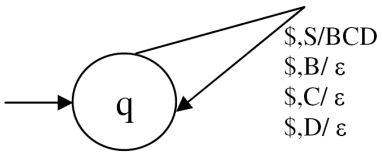
State	*Input symbol*	*Transition state*
q_0	$	q_1
q_1	$	q_2
q_2	$	q_3
q_3	$	q_4

Pushdown automata is essentially a finite state machine coupled with the stack to store a string of arbitrary length. Strings generated by context free grammars forms a language called context free language (CFL). Pushdown Automata recognises CFLs. There are two ways in which the strings generated by CFG are accepted by pushdown automata one is by emptying the stack and the other one by entering the accepting state. A PDA formally defined as a seven-tuple M = (Q, Σ, S, δ, q_0, Z_0, F), where Q is the finite number of states, Σ is input symbols, S is stack symbols, $\delta: Q \times (\Sigma \cup \{\varepsilon\}) \times S \rightarrow Q \times S^*$ is the transition function, $q_0 \in Q$ is the initial state, $Z_0 \in S$ is the initial stack top symbol, $F \in Q$ is a set of accepting states (https://www.walesonline.co.uk/business/personalfinance/hole-wall-machine-50-years-13242356).

Transition function of pushdown automata recognising ATM PIN generated by context free grammar is as follows:

δ(q, 0, S) = (q, BCD), δ(q, 1, S) = (q, BCD),
δ(q, 2, S) = (q, BCD), δ(q, 3, S) = (q, BCD),
δ(q, 4, S) = (q, BCD), δ(q, 5, S) = (q, BCD),
δ(q, 6, S) = (q, BCD), δ(q, 7, S) = (q, BCD),
δ(q, 8, S) = (q, BCD), δ(q, 9, S) = (q, BCD),
δ(q, 0, B) = (q, ε), δ(q, 1, B) = (q, ε),
δ(q, 2, B) = (q, ε), δ(q, 3, B) = (q, ε),
δ(q, 4, B) = (q, ε), δ(q, 5, B) = (q, ε),
δ(q, 6, B) = (q, ε), δ(q, 7, B) = (q, ε),
δ(q, 8, B) = (q, ε), δ(q, 9, B) = (q, ε),
δ(q, 0, C) = (q, ε), δ(q, 1, C) = (q, ε),
δ(q, 2, C) = (q, ε), δ(q, 3, C) = (q, ε),
δ(q, 4, C) = (q, ε), δ(q, 5, C) = (q, ε),
δ(q, 6, C) = (q, ε), δ(q, 7, C) = (q, ε),
δ(q, 8, C) = (q, ε), δ(q, 9, C) = (q, ε),
δ(q, 0, D) = (q, ε), δ(q, 1, D) = (q, ε),
δ(q, 2, D) = (q, ε), δ(q, 3, D) = (q, ε),
δ(q, 4, D) = (q, ε), δ(q, 5, D) = (q, ε),
δ(q, 6, D) = (q, ε), δ(q, 7, D) = (q, ε),
δ(q, 8, D) = (q, ε), δ(q, 9, D) = (q, ε).

Figure 2 Pushdown automata recognising generated ATM PIN



6 Implementation process

Once the regular grammar/context free grammar is ready to be applied for generation of ATM PIN, the operation tool to implement could be optimised as below.

1 Open/launch the accessing tool for string generation (PIN).

2 On the login screen, the authorised admin user enters his credentials for generating PINs.

3 Tool launches its main page and request for data to be stored as customer ID, account ID and ATM card number.

4 User enters all these data which is stored and maintained in the database for generating ATM PIN.

5 User can view the table to identify all account IDs for which ATM PIN has been generated and for which yet to be generated.

6 Admin user can trigger the grammar either regular grammar/context free grammar which picks up each record with ATM PIN field blank and generates the PIN one-by-one.

7 Each record with customer ID, account ID and ATM card number would ultimately have a generated PIN which would be printed and delivered to customer.

8 On login to ATM with the card, when customer enters the ATM PIN given for the account the server verifies the PIN against that in tool record and confirms Yes, to proceed.

9 If customer changes the ATM PIN anytime, the server process and completes the PIN change request, saves the new PIN in encrypted form in the tool for data maintenance and authorisation. This should not impact the PIN generation process.

   Once the customer request for reset of the ATM PIN due to

   - Auto expiry: post the valid hours, the ATM PIN set to null, hence the grammar can just be run to create a new PIN.
   - Locked state: post the user locking the PIN, manually the bank/institution should unlock the ATM card PIN, reset the PIN to null state and then run the grammar.

10 When the user enters PIN, the system will direct the entered PIN to database of the administrator, where it will recognised by finite state machine or pushdown automata and then authorisation will be granted.

7 Conclusions

The essential destination of this exploration is to create and to outline a framework to produce ATM PIN number quick, dependable, compelling and productive. The created framework can be bundled and enhanced to turn into a standard one that can be extensive use for business operations. To understand this nonetheless, there is a need to do exercises, for example, data test, user acknowledgement testing, system review and deployment. The recorded techniques in this paper are likewise great wellspring of data for further framework advancement and information investigation. This paper paves a novel way to generate ATM PIN using mathematical and computational model. the computation process is simple, faster and cost-effective for the generation of PINs with this automated computation method.

7.1 Future work

As a mathematical model this proposed PIN generation technique can be implemented for effective functioning. Service provider point of view the proposed technique can be implemented tested for its optimality.

References

Akomolafe, D.T. and Afeni, B.O. (2014) 'Using database management system to generate, manage and secure personal identification numbers (PIN)', *Journal of Software Engineering and Applications*, Vol. 7, No. 5, pp.461–469.

Babatunde, I.G. and Charles, A.O. (2013) 'A fingerprint-based authentication framework for ATM machines', *Journal of Computer Engineering & Information Technology*, Vol. 2, No. 3, doi:10.4172/2324-9307.1000112.

Bond, M. and Zielinski, P. (2003) *Decimalisation Table Attacks for PIN Cracking*, Technical Report, University of Cambridge, No.560.

Hopcroft, J.E. and Ullman, J.D. (1979) *Introduction to Automata Theory*, *Languages*, *and Computation*, Addison-Wesley.

Irish, V (1998) 'Engineering communications from St. Columba to the internet', *Engineering Management Journal*, Vol. 8, No. 5, pp.221–228.

Karovaliya, M., Karedia, A., Oza, S. and Kalbande, D.R. (2015) 'Enhanced security for ATM machine with OTP and facial recognition features', *Procedia Computer Science*, Vol. 45, pp.390–396.

Lee, M-K., Nam, H. and Kim, D.K. (2016) 'Secure bimodal PIN-entry method using audio signals', *Computers & Security,* Vol. 56, No. C, pp.140–150.

Scarfo, P. (2017) 'Biometrics at the ATM', *Biometric Technology Today*, Vol. 2017, No. 1, pp.9–11.

Stanekova, L. and Stanek, M. (2013) 'Analysis of dictionary methods for PIN selection', *Computers & Security*, Vol. 39, No. B, pp.289–298.

Wu, W. (2011) 'The research and design of ATM PIN pad based on triple DES', *IEEE International Conference on Information and Automation* (*ICIA*), Shenzhen, pp.443–447.

Websites

http://www.investorwords.com/3684/personal_identification_number.html#ixzz399wdZEU6.

http://www.knowledgehub.co.in/2010/07/meaning-ofnumbers-on-debit-credit-card.html.

https://banking.about.com/od/checkingaccounts/g/pinnumber2.htm2.

https://banking.about.com/od/securityandsafety/p/pinnumber.htm.

https://hackedgadgets.com/2006/12/01/atm-pinnumbers-hacked/.

https://homesecurity.about.com/od/online/fl/Using-PINs-Safely.htm.

https://inventors.about.com/od/astartinventions/a/atm_2.htm.

https://tr.cyclopaedia.net/wiki/Finite-state_machine.

https://whatis.techtarget.com/definition/finite-statemachine.

https://www.engineersgarage.com/inventionstories/atm-history.

https://www.techopedia.com/definition/12128/personal-identification-number-pin.

https://www.walesonline.co.uk/business/personalfinance/hole-wall-machine-50-years-13242356.