

OTP Generation Using LFSR To Validate Applicant Login Account

Manoj Kumar¹, Karthik Shakyawar², Navin³

^{1, 2, 3}*Department of ECE, NIT Manipur, Langol, Imphal, Manipur, India 795004*
Email: ¹manojara400@gmail.com

Most of the user login accounts used on web sites and mobile apps are authenticated by using a static password. Static password-based authentication systems are not very secure; they are easy to guess, and users also have to remember them. To avoid this problem, an OTP (one time password)-based password generation system for validating user login accounts is developed in this paper. Three types of 13-bit linear feedback shift register (LFSR) circuits are developed using XNOR gates, and they are synthesized and simulated using the Xilinx Vivado 2015.2 tool. Proposed LFSR circuits do not use any initial seed value, and they generate random numbers at a frequency of 200 MHz. Random numbers generated by LFSR circuits are written to text files, and four characters of decimal digits are used to generate an OTP. In this work, two forms are developed by the Anvil tool, where the user has to enter his email address, date of birth, and OTP to login to the system. The Anvil tool randomly selects the four-character OTP from the text file, and it is sent to the user's email address for validating their login accounts. Developed LFSR circuits consume area (LUTs) in the range of 1-2, and they consume 0.192W–0.193W of power.

Keywords: OTP, LFSR, RNG, VHDL, Anvil

I. INTRODUCTION

Today, the Internet is used everywhere, and our data is shared globally. Our shared information over the internet must be protected from unauthorized access. Users are registering on various internet-based sites or apps to take advantage of faster processing of their needs. For registering on these sites or apps, the user has to enter his basic details, and he has to create a text password for entering these sites. For creating text-based passwords, users have to use characters, decimal numbers, and symbols [1]. Text passwords are the simplest and most widely used, but they are not highly secure. Also, users can forget or lose these types of passwords. To solve this issue, a one-time password (OTP) was developed by Leslie Lamport [2]. OTP can be used to enhance the security of user authentications [3]. Also, OTPs are used to eliminate manual password creation and management. Each generated OTP can be used in a single instant of time [4]. OTP can be used for web-based or mobile phone applications. OTP is random data, and it can be generated by either hardware architecture or software. Compared to OTP generated by software, hardware-based OTP is more reliable and secure. Random Number Generator (RNG) architectures are used to generate random numbers, and they can be used in OTP generation. Anvil is a very simple, easy-to-use tool for building any type of

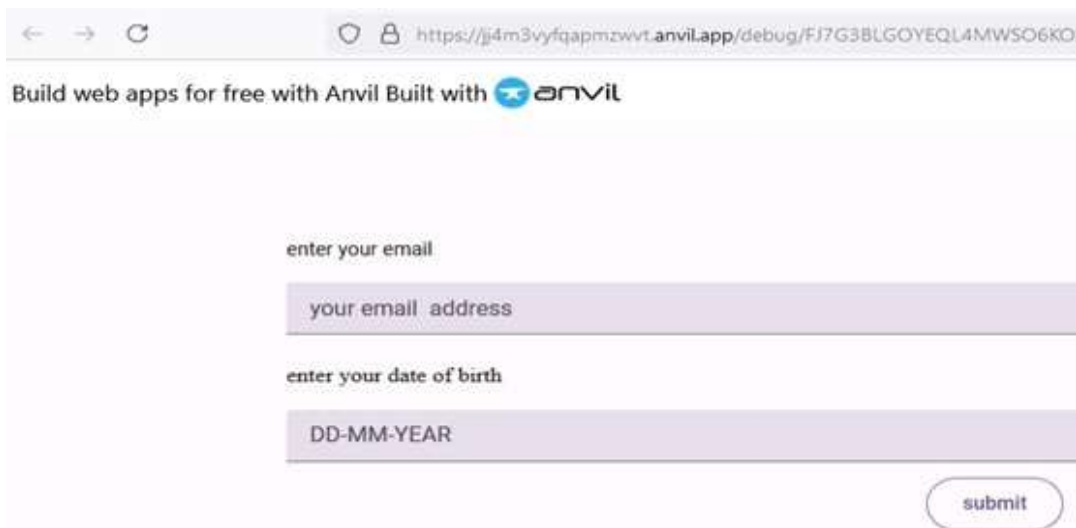
web- application [5]. This research worked on developing various random number generator architectures using LFSR (Linear Feedback Shift Registers) circuits, and these random numbers were used for generating OTP. In this work, Anvil is used for creating an applicant login account form and validating this login account by using the generated OTP.

II. RELATED WORK

Many authors have been working on generating OTP based on hardware and software approaches and using the generated OTP for building web- applications or mobile apps. Eddy Prasetyo Nugroho et al. [6] use OTP and the Advanced Encryption Standard (AES) to generate SMS authentication codes. The generated SMS code was used to open a new applicant account and to minimize the creation of fake and rough accounts. The disadvantage of this method is its higher time consumption compared with the existing standard AES-256 algorithm. To access a web-based academic information system, the authors in their paper [7] use OTP, SMS Gateway, and MD5 hash encryption algorithms. In this work, the authors have developed a secure login system, and an OTP was sent automatically to registered student mobile numbers. The OTP mutual authentication scheme was developed by Muhammad Taufiq and Dion Ogi in 2018 [8]. Here, the authors have used a Raspberry Pi to implement a client-server-based room access control system. Shakir M. H. Al-Farraj and Huda K. Saadeh [9] provide a new method to generate OTP by using user identity and the timestamp. By using this information, a string is created, which is used to generate random permutations of a given size. Different sizes of OTP are generated by using this random permutation. A new method for generating six-character OTP based on a linear congruential generator (LCG) was proposed by Imamah in 2018 [10]. For generating OTP, first plaintext containing user information such as username, mobile number, and access time is encrypted using the AES 256 algorithm, and then encrypted text is randomized using LCG to generate OTP. Yun Huang et al. [11] proposed a new OTP method and its application in a mobile phone two-factor authentication prototype. A security login system with OTP was developed on an FPGA by the authors in a paper [12]. The authors in the paper [13] studied SMS OTP authentication protocols in Android apps. A new OTP method based on the changed location and angle of fingerprint features was proposed by Byung-Rae Cha et al. [14]. Paper [15] provides a service where OTP can be accessed from any web account. In this work, an assigned set of keys is encrypted to generate an OTP. The authors in the paper [16] developed a security system by using a hybrid cryptography method based on OTP-RSA. The Java environment is used to run this system. The proposed system provides a very strong security system for the documents stored in the cloud. In [17], a secured hash algorithm (SHA1) is used to generate an OTP for implementing a two-factor authentication system on smartphones. In this work, a server- and client-side GUI are developed using an Android program. A design framework for the locker security system was developed using OTP, IOT, and face recognition by the authors in a paper [18]. The proposed locker system was accessible either by using an OTP, locker password, or both.

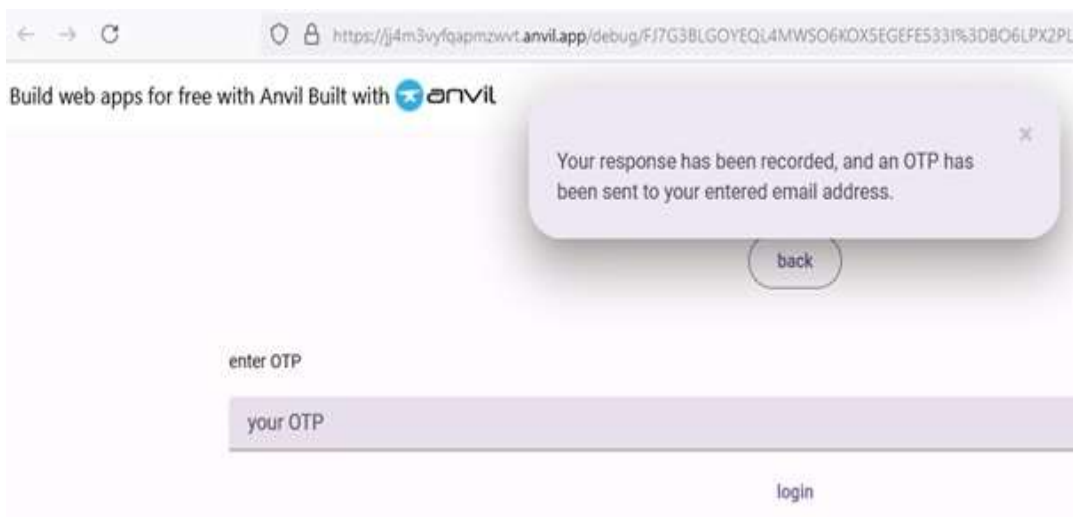
III. PROPOSED APPLICANT LOGIN SYSTEM

To validate the applicant login account, two forms (Form1 and Form2) are created by the Anvil tool. In these forms, the user has to enter his registered email address, date of birth, and OTP. Form1 and Form2 are shown in Figures 1 and 2, respectively. To use this system, users have to first register in it, and then they can access it without using a plaintext password. A flowchart for the proposed applicant login system is shown in Figure 3.



The screenshot shows a web browser window with the URL <https://jj4m3vyfqapmzwwt.anvil.app/debug/F17G3BLGOYEQL4MWSO6K0X>. The page header says "Build web apps for free with Anvil Built with anvil". The form contains two input fields: "enter your email" with a placeholder "your email address" and "enter your date of birth" with a placeholder "DD-MM-YEAR". A "submit" button is located at the bottom right.

Figure.1:Form1 picture developed by Anvil tool



The screenshot shows a web browser window with the URL <https://jj4m3vyfqapmzwwt.anvil.app/debug/F17G3BLGOYEQL4MWSO6K0X5EGEF5331%3D806LPX2PL>. The page header says "Build web apps for free with Anvil Built with anvil". A success message box says "Your response has been recorded, and an OTP has been sent to your entered email address." with a "back" button. Below the message is an "enter OTP" label and a "your OTP" input field. A "login" button is at the bottom right.

Figure.2:Form2 picture developed by Anvil tool

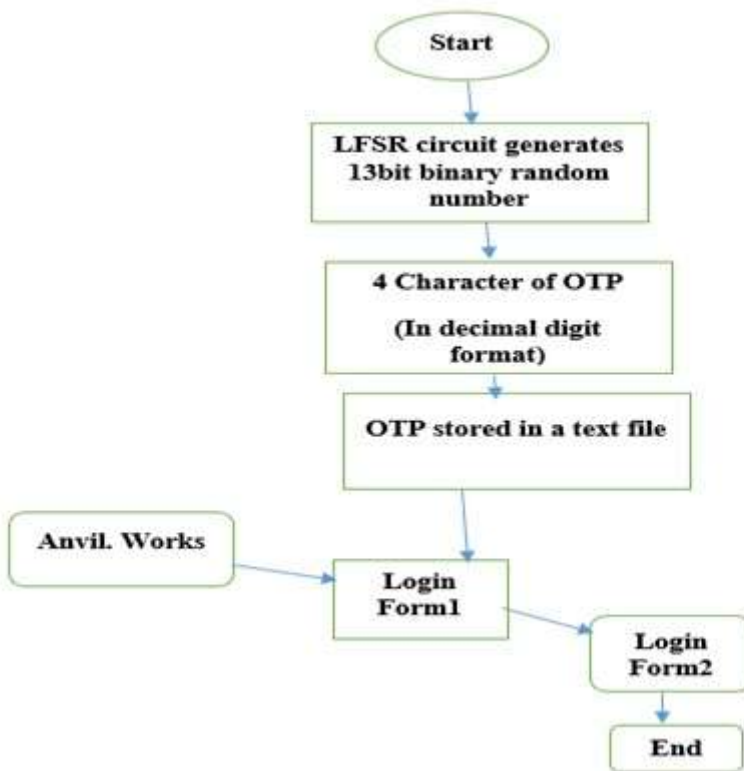


Figure.3: Flowchart for the proposed applicant login system

The detail description for Figure.3 is as follows:

- The LFSR circuit generates a 13- bit binary random number.
- If 13- bit binary number value is greater than 1000, then that number is used for generating 4 characters OTP.
- The Generated 4 characters OTP are written into a text file.
- The Server side program randomly sends 4 characters OTP to the user's email address.
- After entering OTP in login form 2, an email is sent to inform the user about their login status.

Four characters OTP in decimal digits format is send to user's registered email address automatically after clicking submit button in the login form1. Also, a message is also displayed for some instant of time , informing the user about an email sent to their email address. The user enter four characters of OTP in the login form2. And a message" Check your email." is displayed after clicking login button in form2. If a valid OTP is entered in login form2, then a message"Login is successful." is send to user email address. If an invalid OTP is entered in login form2, then a message "Login is not successful." is send to user's email address.

3.1 LFSR

LFSR is cascaded connections of flip-flops and it uses feedback to generate a sequence of binary random numbers [19]. Generated random numbers from the LFSR circuit can be used in Cryptography, gambling, generating pseudo-random numbers and mobile and space communications. Random number generated by LFSR circuits depends on three factors 1. Polynomial 2. logic gates (either XOR or XNOR) 3. Feedback style [20]. In this work, three types of LFSR circuits are developed for generating OTP and they are discussed below.

3.1.1 13 bit Simple LFSR

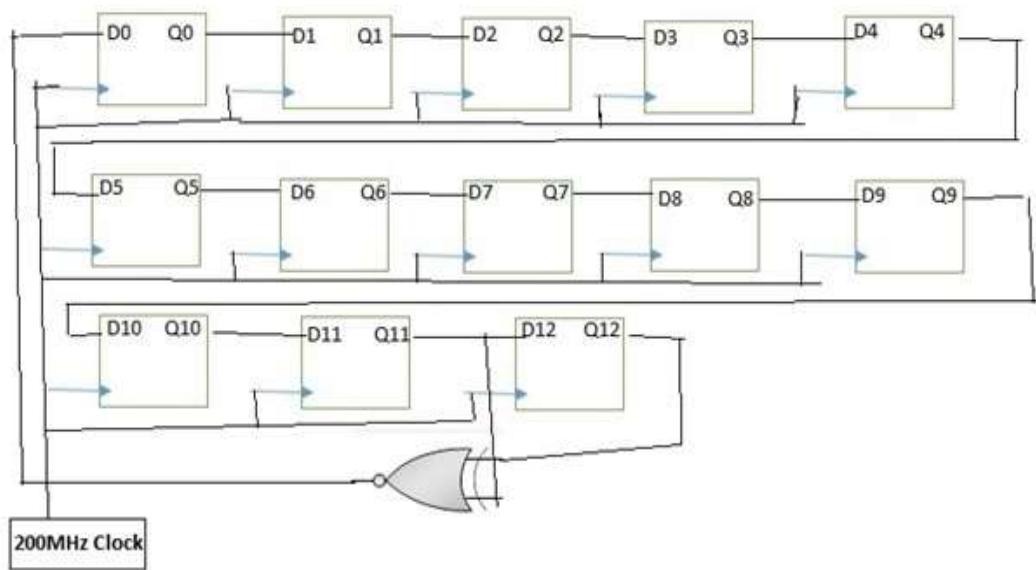


Figure.4: 13- bit simple LFSR circuit diagram

A circuit diagram for simple 13 bit LFSR is shown in Figure.4. Feedback polynomial for this LFSR circuit is $X^{12} + X^{11} + 1$ and it generates $2^{13} - 1 = 8191$ random outputs [21]. This circuit uses one XNOR gates and it is connected between 12th and 13th Flip-Flops. Output of XNOR gate is connected to input of the first Flip-Flop. This circuit does not use any seed value. For generating 13 bit random number outputs of all Flip-Flops are considered.

3.1.2 13 bit Fibonacci LFSR

A 13 bit Fibonacci LFSR circuit diagram is shown in Figure.5. Here, Tap (bit positions) affects the next state are [12, 11, 9, 8]. Feedback polynomial for this diagram is $X^{12} + X^{11} + X^9 + X^8 + 1$. In this polynomial X^0 does not indicate any Tap value but it corresponds to the input to the first Flip-Flop. In this circuit, Taps are XNORed sequentially with rightmost bit and then feedback into the leftmost bit [22].

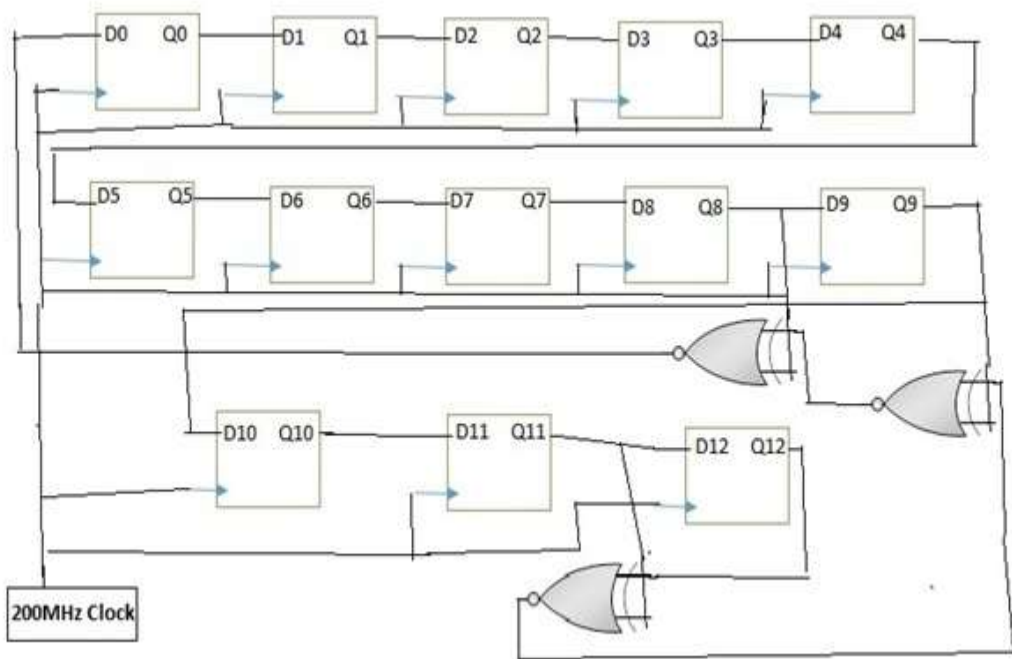


Figure.5: 13-bit Fibonacci LFSR circuit diagram

Combined RNG architecture using LFSR

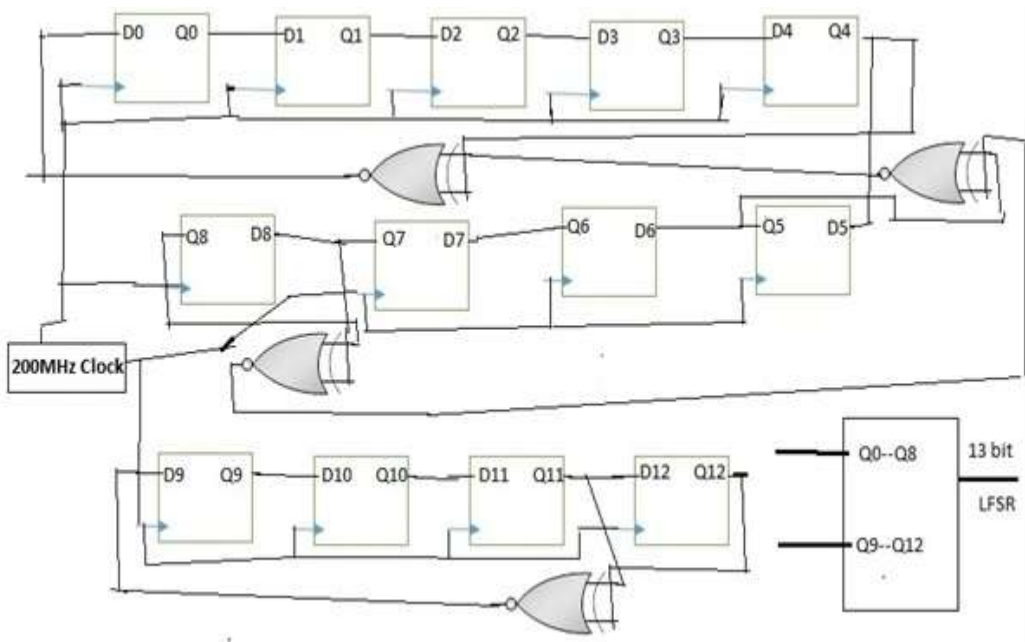


Figure.6: Combined RNG architecture using LFSR circuit

A combined RNG architecture using LFSR circuit is shown in Figure.6. Here, 9-bit and 4-bit LFSR circuits are combined to generate 13 bit random numbers [23]. Feedback polynomial for 9-bit LFSR circuit is $X^8+X^7+X^5+X^4+1$ and for 4bit LFSR circuit it is $X^{12}+X^{11}$. Figure.6 uses 4 XNOR gates to form the combined RNG architecture. Flip-Flops output from Q0-Q8 and Q9-Q12 is taken to generate 13 bit random numbers.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

All three types of LFSR circuits are designed using VHDL (Very High Speed Integrated Circuit HDL) and implemented on an Artix 7 FPGA (7a35t-cpg236) device. Xilinx Vivado 2015. 2 tools are used to synthesize, simulate, and create text files with four characters of OTP. LFSR circuits operate at a 200 MHz clock frequency, and this frequency is generated by using the IP Catalog->FPGA Features And Design->clocking->clocking wizard of Vivado 2015. 2 tool. Generated OTP from LFSR circuits is saved in a text file by using VHDL testbench program (by using STD.TEXTIO package). Anvil tool is used to create client-side login forms 1 and 2. Also, server-side code is written to randomly send OTP to the user email address and display messages. An experimental output for login forms 1 and 2 is shown in Figures 7 and 8, respectively.



Figure.7: Login Form1 experimental output

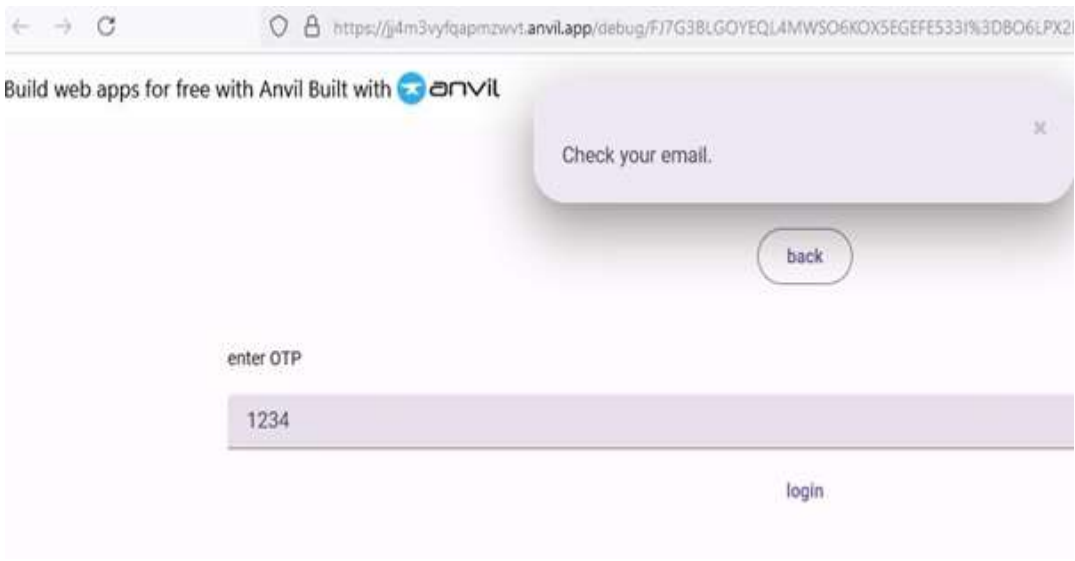


Figure.8: Login Form2 experimental output

The RTL schematic diagram for the designed LFSR circuits is shown in Figures 9, 11, and 13, respectively. Simulation output waveforms for the developed LFSR circuits are shown in Figures 10, 12, and 14, respectively. In these figures, clk represents a 100MHz FPGA system clock, rst represents a reset signal, clkout represents a 200MHz clock, and q[12:0] represents a 13-bit random output signal for the developed random number generator architectures. From 13-bit random output, four characters of OTP in decimal-digit format are stored in a text file. Figure.15 represents an email sent picture with OTP information sent by anvil tool for the user who has successfully entered his details in the login form. Figure.16 represents an email sent picture with login status information sent by anvil tool for the user who has successfully entered his OTP details in the login form 2. If the valid OTP is entered in login form 2, then the Anvil tool sends an email to the user with the message "Login is successful.". If the entered OTP does not match with the sent OTP, then the Anvil tool sends an email to the user with the message "Login is not successful.". Synthesis results comparison among designed LFSR circuits is shown in Table I. From this table, it is clear that a combined RNG architecture using LFSR circuits has higher speed in comparison with the existing LFSR circuits. Proposed 13-bit simple LFSR and Fibonacci LFSR circuits consume less area in comparison with the proposed combined RNG architecture. Also Proposed 13-bit simple LFSR and Fibonacci LFSR circuits consume less area in comparison with the existing LFSR circuits. The proposed 13-bit simple LFSR circuit consumes more power than the proposed 13-bit Fibonacci LFSR and combined RNG circuit. In comparison with Paper [24], [20] and Paper [25] proposed RNG architectures consume less area (in terms of LUTs) and power (in watts).

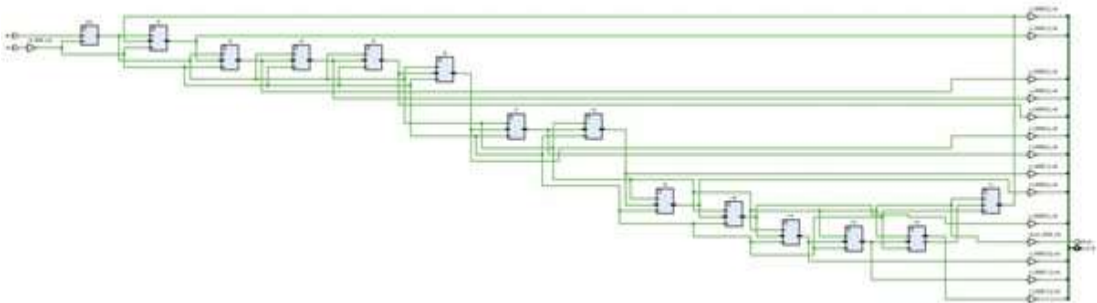


Figure.9: RTL diagram of a 13-bit simple LFSR circuit

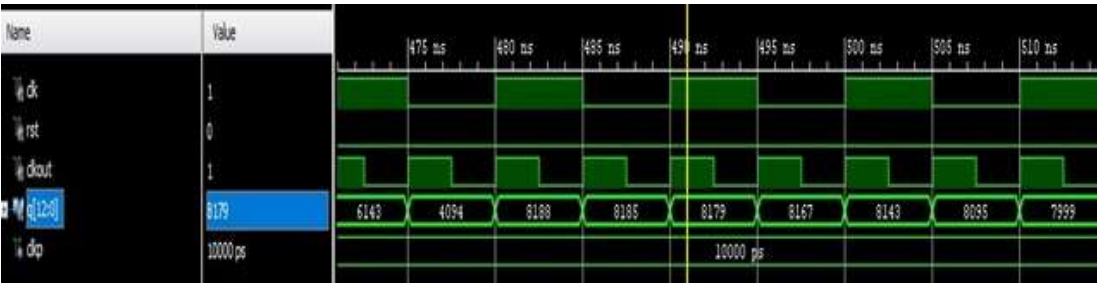


Figure.10: Simulation output waveform of the 13-bit simple LFSR circuit

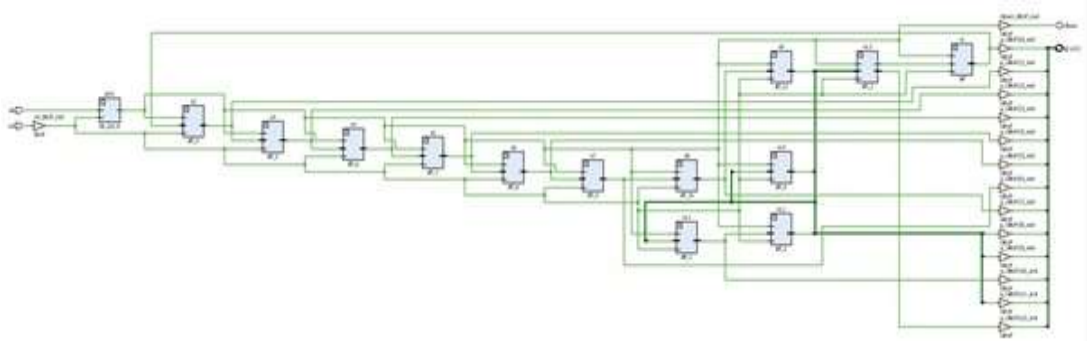


Figure.11: RTL diagram of 13 bit Fibonacci LFSR circuit

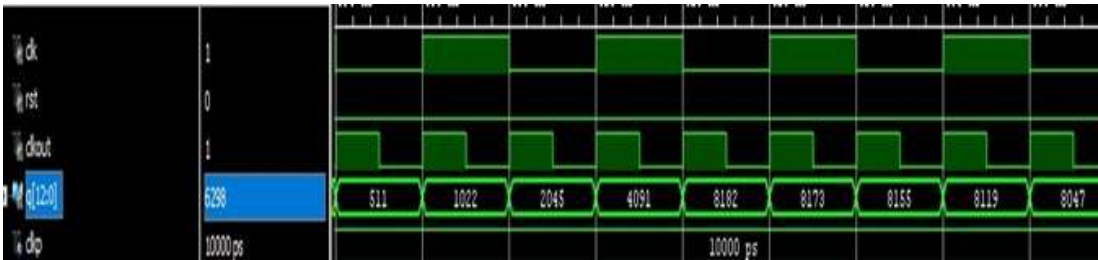


Figure.12: Simulation output waveform of the 13-bit Fibonacci LFSR circuit

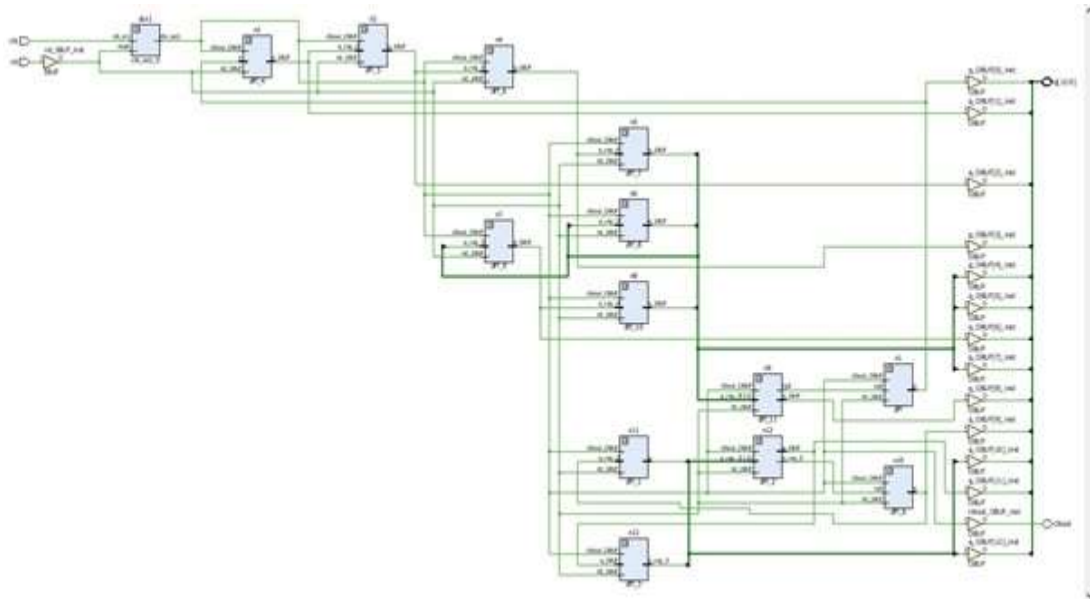


Figure.13: RTL diagram of Combined RNG architecture using LFSR circuit

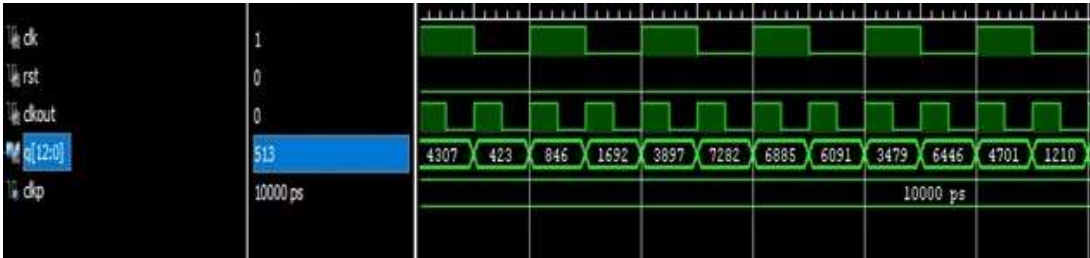


Figure.14: Simulation output waveform of the combined RNG architecture using the LFSR circuit



Figure.15: Email sent with OTP information to the user

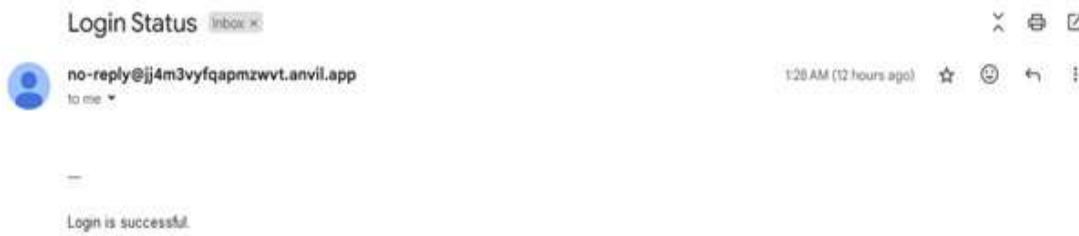


Figure.16: Email sent with login status information to the user

Table. I: Synthesis results comparison among designed LFSR circuits

LFSR Circuit	Device	Area(in terms of LUTs)	Speed(ns)	Total on chip Power Consumption(watts)
Proposed 13 bit simple LFSR circuit	7a35t-cpg236	1	1.155	0.193
Proposed 13 bit Fibonacci LFSR circuit	7a35t-cpg236	1	1.562	0.192
Proposed Combined RNG architecture using LFSR circuit	7a35t-cpg236	2	1.403	0.192
Jitter based LFSR[20]	Virtex-5	5	2.129	

Bit swapping LFSR using BIST[20]	Virtex-5	9	2.309	
Multibit LFSR[24]	Spartan6	16	1.507	
Cellular automata with LFSR[25]	Spartan3E	8	9	
Cellular automata LFSR[20]	Virtex-5	3	2.309	

V. CONCLUSION

Different types of LFSR circuits using VHDL are designed and implemented on an Artix 7 FPGA device. Four-character OTP in decimal-digit format are generated from the designed LFSR circuits. Simulation output waveforms for the designed LFSR circuits clearly show 13-bit random number output. RTL diagrams for the developed LFSR circuits are shown. Anvil tool is used to create client and server side architecture for the proposed login system. Combined RNG architecture using LFSR circuits has higher speed than the implemented LFSR circuits. Proposed LFSR circuits consume less area and power. Also proposed LFSR circuits operate at very high clock speed. Anvil tool randomly sends OTP to the user, and there is no chance of OTP repetition. Generated OTP is highly secure, and registered users do not have to remember any plaintext password for using this login system. Designed RNG architectures with OTP information can be used in developing web sites, mobile apps, cryptography, security systems, etc. In the future, after successful login, the user homepage of the web sites or mobile apps can be created to make this system more real-time.

Acknowledgements The authors would like to thank Dr Manoj Kumar for his complete support and guidance.

Data Availability No datasets were generated or analysed during the current study.

Funding Not Applicable.

Declarations

Competing Interests The authors declare no competing interests.

References

1. Imamah, A. Djunaidy and a. et, "Comparasion of Password Generator between Coupled Linear," in IOP Conf. Series: Journal of Physics: Conf. Series 953 , Bali, 2017.
2. L. Lamport Password Authentication with Insecure Communication, In: Comm. ACM, vol. 24, No 11, 1981, pp. 770-772.

3. M. J. Kim, B. H. Lee, and S. J. Kim, "Weakness and Improvements of a One-time Password Authentication Scheme," *International Journal of Future Generation Communication and Networking*, vol. 2, no. 4, pp. 29-39, 2009.
4. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1996.
5. <https://anvil.works/docs/overview>.
6. Eddy Prasetyo Nugroho, Rizky Rachman Judhie Putra, Iman Muhamad Ramadhan," SMS Authentication Code Generated by Advance Encryption Standard (AES) 256 bits Modification Algorithm and One Time Password (OTP) to Activate New Applicant Account",In proc of 2nd International Conference on Science in Information Technology (ICSITech),IEEE,.pp.175-180,2016.
7. Eko Sedyono, Kartika Imam Santoso and Suhartono," Secure Login by Using One-time Password Authentication Based on MD5 Hash Encrypted SMS ",In proc. of International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE,pp.1604-1608,2013.
8. Muhammad Taufiq and Dion Ogi," Implementing One-Time Password Mutual Authentication Scheme on Sharing Renewed Finite Random Sub-Passwords Using Raspberry Pi as a Room Access Control to Prevent Replay Attack",In proc. of International Conference on Electrical Engineering and Informatics (ICELTICs), IEEE,Sept. 19-20, 2018.
9. Shakir M. H. Al-Farraj and Huda K. Saadeh," One Time Password Generation based on Random Permutation using User Identity with Timestamp", *International Journal of Engineering and Advanced Technology (IJEAT) IS*, Volume-9 Issue-4, April 2020.
10. Sudha Anbalagan, Gunasekaran Raja, Kottilingam Kottursamy, Guggilam Swetha Aparna, Jeyalakshmi Kumaresan, Mansoor Ihsan, "Authorized Arming and Safeguarded Landing Mechanisms for Drones", 2020 IEEE Globecom Workshops (GC Wkshps), pp.1-6, 2020.
11. Yun Huang, Zheng Huang, Haoran Zhao, Xuejia Lai," A new One-time Password Method",In proc. of International Conference on Electronic Engineering and Computer Science, IERI Procedia, Vol.4, pp.32-37,2013.
12. Samiksha Subba, Bhawana Dahal, Nirmal Rai, Rochan Banstola, Suman Das, Surya Prakash Tamang," FPGA based Security Login System using GSM with OTP Generation", *International Journal of Advanced Engineering Research and Science (IJAERS)*, Vol-4, Issue-2, Feb- 2017.
13. MA, Siqi; FENG, Runhan; LI, Juanru; LIU, Yang; NEPAL, Surya; BERTINO, Elisa; DENG, Robert H.; MA, Zhuo;and JHA, Sanjay,"An empirical study of SMS one-time password authentication in Android apps", *Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC 2019)*. 339-354,2019.
14. ByungRae Cha, KyungJun Kim and HyunShik Na, "Random password generation of OTP system using changed location and angle of fingerprint features," 2008 8th IEEE International Conference on Computer and Information Technology, Sydney, NSW, Australia, 2008, pp. 420-425.
15. Florêncio, D., Herley, C. ," One-Time Password Access to Any Server without Changing the Server". In: Wu, TC., Lei, CL., Rijmen, V., Lee, DT. (eds) *Information Security. ISC 2008. Lecture Notes in Computer Science*, vol 5222. Springer, Berlin, Heidelberg, 2008.
16. Karthik, Chinnasamy, and Deepalakshmi," Hybrid Cryptographic Technique Using OTP:RSA",In proc. of International Conference on Intelligent Techniques In Control, Optimization And Signal Processing,IEEE,2017.
17. Sagar Acharya, Apoorva Polawar and P.Y.Pawar," Two Factor Authentication Using Smartphone Generated One Time Password", *IOSR Journal of Computer Engineering (IOSR-JCE)*, 8727Volume 11, Issue 2 (May. - Jun. 2013), PP 85-90.
18. N. Anusha, A. Darshan Sai and B. Srikar," Locker Security System Using Facial Recognition and One Time Password (OTP)",In proc. of WiSPNET 2017 conference,IEEE,pp.812-815,2017.

19. Huirem Bharat Meitei and Manoj Kumar,” FPGA-Based True Random Number Generator Architecture Using 15-Bit LFSR and ADPLL”, . In: Swain, B.P., Dixit, U.S. (eds) Recent Advances in Electrical and Electronic Engineering. ICSTE 2023. Lecture Notes in Electrical Engineering, vol 1071. Springer, Singapore. https://doi.org/10.1007/978-981-99-4713-3_27.
20. B.Murali Krishna, G.L.Madhumati, Habibulla Khan,” FPGA based Pseudo Random Sequence Generator using XOR/XNOR for Communication Cryptography and VLSI Testing Applications”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-4, February 2019.
21. Shruti Hathwalia and Meenakshi Yadav,” Design and Analysis of a 32 Bit Linear Feedback Shift Register Using VHDL”, Int. Journal of Engineering Research and Applications, Vol. 4, Issue 6, pp.99-102 June 2014.
22. Vishakha V. Bonde and A. D. Kale,” Design and Implementation of a Random Number Generator on FPGA”, International Journal of Science and Research (IJSR), Volume 4 Issue 5, May 2015.
23. W.A.S Wijesinghe, M.K Jayananda and D.U.J Sonnadara,” Hardware Implementation of Random Number Generators”, Proceedings of the Technical Sessions Institute of Physics – Sri Lanka, Vol.22 , pp.28-38,2006.
24. D. Datta, B. Datta and H. S. Dutta, "Design and implementation of multibit LFSR on FPGA to generate pseudorandom sequence number," 2017 Devices for Integrated Circuit (DevIC), Kalyani, India, 2017, pp. 346-349.
25. David H. K. Hoe, Jonathan M. Comer, Juan C. Cerda, Chris D. Martinez, Mukul V. Shirvaikar,” Cellular Automata-Based Parallel Random Number Generators Using FPGAs”, International Journal of Reconfigurable Computing, Volume 2012, Article ID 219028,2012.