FPGA Implementation of RC-4T and WPA

Ravi Kishore Kodali, Satya Kesav Gundbathula and Lakshmi Boppana
Department of Electronics and Communication Engineering
National Institute of Technology, Warangal
WARANGAL, 506004 INDIA

***Abstract*—Security is an important feature to be included in the field of wireless communications, where the transmission and reception need to be unassailable. Every wireless device needs to adopt a security model which may be complex or simple to make the communication impregnable. The algorithm to be chosen for the final implementation depends on the characteristics of the device. Applications requiring higher security should employ devices having computational capabilities and good amount of hardware and those applications that do not need to have tight security can compromise with the hardware resources and the ability of the micro-controller/microprocessor. In this work two security models namely, the RC-4 with the *Toeplitz* hash algorithm (RC-4T) and the Wi-Fi protected Access (WPA) have been compared in terms of hardware complexity and combinational delay. Both of these algorithms have been implemented using the *Xilinx Virtex-6q* FPGA device for the comparison based on resource utilization and delays. *Toeplitz* hash function has been used along with RC-4 algorithm for the generation of the key stream thus making the security model more robust as compared to the traditional WEP.**

***Index Terms*—Stream cipher, Hash function, *Toeplitz*, WEP, WPA**

I. Introduction

Physical devices require communication links which may be either wired or wireless. Several attacks such as eavesdropping, denial of service, unauthorized access may take place with wireless connectivity. Hence, the wireless devices have to make use of a cryptographic security model to secure against such type of attacks. Various devices can make use of different cryptographic algorithms depending on the resources such as computational power, memory, energy source available with the devices and the security model demanded by the application. Two simple models are: *wired equivalent privacy* (WEP) and *Wi-Fi protected access* (WPA). The same key, which is static, is used for encryption and decryption in WEP and it can be easily broken as the static key that is generated during its simple operation [1]. WPA has been developed to overcome the weaknesses of the WEP protocol [2]. WPA uses the *Temporal key integrity protocol* (TKIP) along with RC-4, a stream cipher, which makes it more reliable and superior [3]. TKIP uses the physical or MAC address of the device for its operation and make the intermediate key unique, even when a duplicate temporal key is inadvertently used. This work proposes *Toeplitz* hash function for the generation of dynamic key to be used along with the RC-4 stream cipher. The *Toeplitz* hash function is used to compute a secret dynamic key using a public key. A key stream is generated by RC-4. This key stream is used during the encryption process. Thus the RC-4 with the *Toeplitz* hash function makes the model more rigid and secure than the WEP. The timing delay and hardware complexity combined together decide the algorithm to be chosen for an application. The WPA and the proposed *Toeplitz* hash based RC-4 have been implemented using FPGA. A comparison of the characteristics and complexity of both the approaches has been made. The rest of the paper is organized as follows: Section II provides the literature survey, section III presents an overview of the cryptographic algorithm RC-4 used along with the *Toeplitz* hash function for the key stream generation and the WPA, the scheme of experimentation is described in section IV, simulation and experimental results are presented in section V and section VI concludes the work.

978-1-4799-6646-2/14/$31.00 ©2014 IEEE

II. Literature review

The *wired equivalent privacy* (WEP) is a simple algorithm with many flaws making the system that uses it insecure [4]. Also, the secret key is static [5]. A modified security algorithm, *d-WEP* is designed to defend against the attacks on the traditional WEP [6]. Wi-Fi Protected Access (WPA), successor to WEP, which has been attacked and is still in use today due to the security needs for applications such as Small Office/Home Office (SOHO) [7]. WPA extends its security complexity and robustness over WEP by using *Temporal key integrity protocol* (TKIP) along with RC-4 for the data encryption, user authentication which is absent in WEP, and a new scheme for data integrity. The detailed operation of the WPA is explained in [8]. The TKIP in WPA uses two phases to construct per-packet key, whereas WEP simply acquires it by concatenating the initialization vector (IV)and the base-key [3]. WPA-2 has been designed in response to the limitations of WPA. It uses counter mode CBC-MAC protocol (CCMP), in place of TKIP and advanced encryption standard (AES) for ciphering the data, instead of RC-4 which proves it to be a more secure algorithm [9]. AES is one of the symmetric key cryptographic algorithms designed for high performance systems, which is complex and rigid to a great extent when compared to WPA and WEP.

On the other hand, in WEP the static key may be made dynamic by using various hash functions thereby making the model more secure compared to the classical algorithm. Hash functions are simple to be implemented in hardware and may also be used for the data integrity in the same algorithm. *Toeplitz* is one of the hash functions which generates dynamic key using the linear feedback shift register (LFSR) approach and the property of the *Toeplitz* matrix.

A *Toeplitz* hash based stream cipher algorithm has been designed and implemented on hardware which is presented in [10]. Such model has a complexity of $O(2^{m+n})$, where the number of bits in the message is $m+n$. The security of the described model has been tested with a known plain-text attack, which proved it to be insecure [11]. In this work, the same *Toeplitz* function uses a public key to generate a hash value, which serves as the secret key for the RC4 stream cipher. A key stream that is generated by the RC-4 with the help of the dynamic secret key which makes the security model very rigid. The key stream is X-OR'ed with the plain text to generate the cipher text.

Field Programmable Gate Arrays (FPGAs) are electronic devices that have large amount of RAM blocks and logic gates. These devices are programmed by the user to implement complex applications that require high computations. By the implementation of different cryptographic algorithms on the FPGAs, the timing delays and also the complexity in terms of hardware utilization [12] can be computed. The implementation cost, power consumption and the area resources can also be found from the *Xilinx* ISE design tool after synthesis. The implementation of AES and WEP on FPGA, given in [13] resulted in the statistics related to the area resources and throughput of 323 CLBs, 177 Mbps for the AES and 750 CLBs, 2.22 Mbps for the WEP respectively.

III. Description of the RC-4 with the *Toeplitz* hash function (RC-4T) and the WPA

A. Stream cipher cryptographic RC-4T algorithm

Wired Equivalent Privacy (WEP) is a cryptographic algorithm developed to provide a secure communication in a wireless LAN (WLAN). Due to the weaknesses of this algorithm, modifications have been made to the WEP to make it more secure. RC-4 with the *Toeplitz* hash function (RC-4T) is one of the modifications to the WEP, using which a secret key is generated dynamically. Instead of using static key, a set of public-keys that are stored in the memory are used during dynamic key generation. The proposed algorithm uses the same major components as in WEP: secret key, an encryption algorithm, initialization vector (IV) and integrity check value (ICV).

In the proposed algorithm, the size of the secret key is 32- bits and this can be altered during the implementation. IV is a fixed length variable data used in the encryption process. It is sent along with the message packet during the key exchange. When a random value is chosen as IV, there may be a probability of collision which should be taken into consideration.

In the proposed model *Toeplitz* hash function is used to generate the secret key. The hash value is calculated with the help of a matrix derived from the public key and a Boolean matrix. An n^{th} degree irreducible polynomial is chosen over GF(2).

An initial binary seed of length n is chosen randomly and is processed through linear feedback shift register (LFSR), which uses the polynomial coefficients to obtain an expanded binary vector. This vector is formed into a *Toeplitz* matrix and multiplied with the public key matrix to obtain the hash value, which is the secret key to the next stage. This key and the IV are concatenated. The IV and the key are used to permute the s-box in the initialization process of the RC-4 encryption stage. Later, the key stream generated from the RC-4 stage is XORed with the plain-text along with the data integrity value. The CRC-32 algorithm is used for the ICV computation. The block diagram for the RC-4T encryption scheme is given in Figure 1. The WEP has many practical disadvantages such as:

1) Forgery of data packets can not be prevented.
2) Replay attacks can not be avoided.
3) Improper use of RC-4 algorithm and the weakness of the keys make it to experience brute-force attacks.
4) Various cryptanalytic methods have been developed to decrypt the data without knowing the key stream.
5) Message modification without the help of encryption keys cannot be resisted.

The WPA has been designed to overcome all of these disadvantages by making use of complex methods. The proposed algorithm, RC-4T, cannot avoid the forgery and replay attacks but the cryptanalytic method of decryption and brute-force attacks can be resisted.

B. Wi-Fi Protected Access

The modified components in WPA are: the TKIP protocol- which is used along with RC-4 in the encryption/decryption processes, the size of secret key- 128- bits, Initialization vector (IV) length - twice the size of that of WEP, and additional MIC computation to avoid the data forgery. The same data integrity algorithm, CRC-32 is used. The extended length of IV reduces the probability of duplications.

1) TKIP: In Temporal Key Integrity Protocol (TKIP), a per-packet key is generated by using two key-mixing phases to make it difficult for an attacker to correlate the key. During the first phase, the temporal key is XORed with the MAC address, which is unique to produce an exclusive intermediate key. During the second phase, this key is used to encrypt the packet sequence number that is derived from the fragmentation of the plain-text into message protocol data units (MPDUs). The encryption

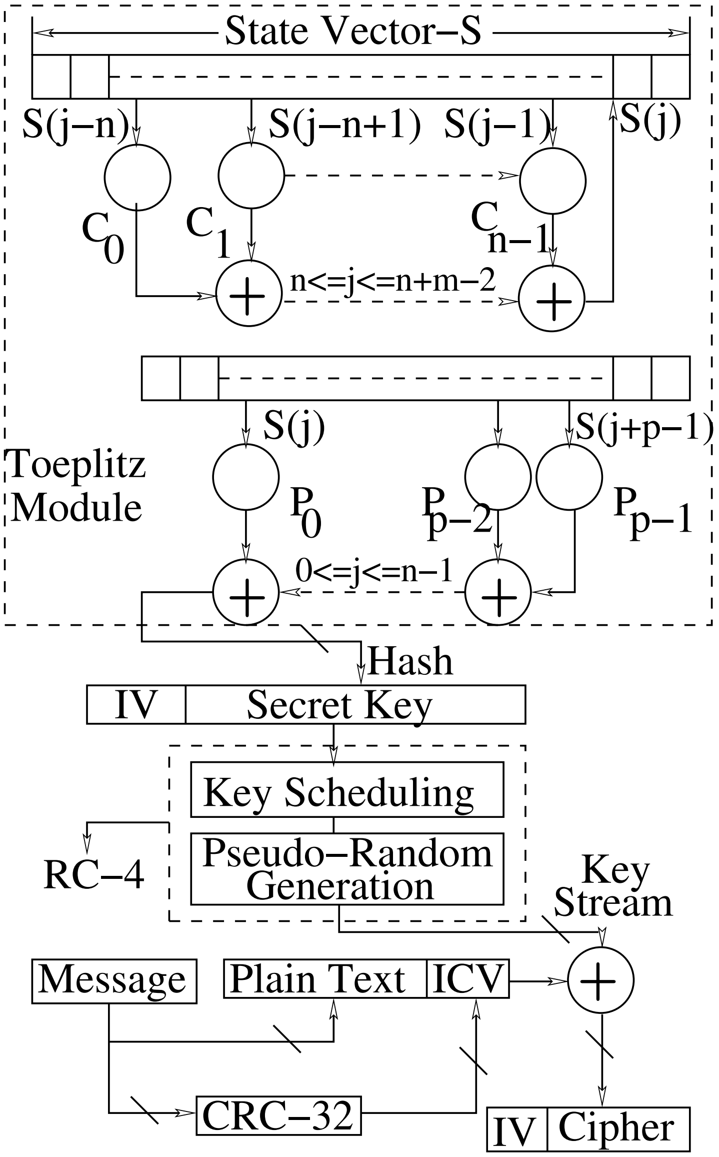

Fig. 1: RC-4T encryption block diagram

stage generates a 128-bit key. This key called the per-packet key and is similar to the key in WEP, where the first 3 bytes correspond to the IV and the next 13 bytes denote the base key.

2) MIC algorithm: The CRC-32 algorithm used in WEP is very weak and is more prone to forgery attempts. Hence *Michael* algorithm, which generates a distinctive message integrity code (MIC), is designed and included with ICV generated by CRC-32 in WPA. The uniqueness of the MIC is achieved by using the MAC address of the system in the computation. The *Michael* algorithm to compute the MIC value is given in Algorithm 1.

3) Encryption/ Decryption stage: The per-packet encryption key generated from the TKIP protocol is used as one of the inputs to the RC-4 stage, which generates the key stream. On the other hand, MIC is calculated from the *michael* key, the source address (SA), destination address (DA), and data using *Michael* algorithm and ICV is calculated using CRC-32 algorithm. The derived key stream is X-ORed with the data, MIC and ICV concatenated together to obtain the encrypted data. The data decryption is done in a similar manner. The block diagram of the WPA encryption is given in Figure 2.

Table I provides a comparison of the characteristics of both the algorithms.

IV. Scheme of Experimentation

Hardware implementation of any algorithm on an FPGA provides the amount of hardware resources it requires, in terms of the number of Look Up Tables (LUTs) and the speed in terms of the combinational delay. In this work, both the approaches have been implemented using *Xilinx*

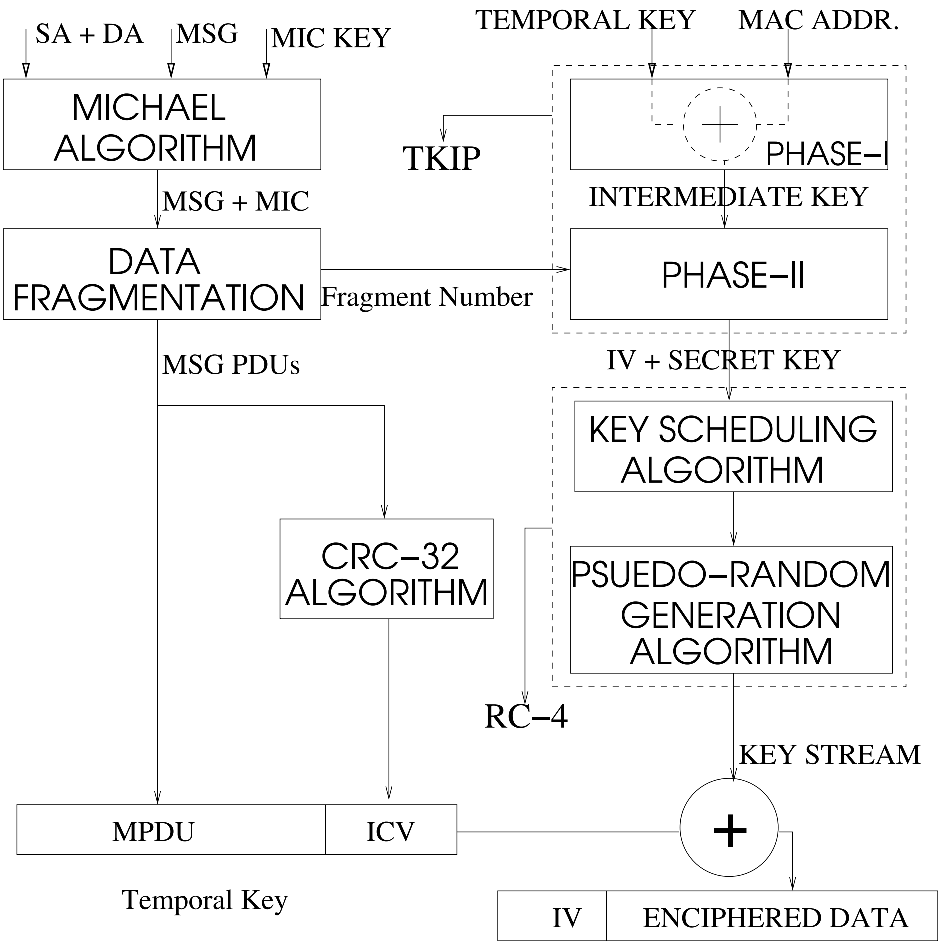

Fig. 2: WPA encryption block diagram

Algorithm 1 Michael algorithm

```
**INPUT** : Michael key $K$ of length 8-bytes and message $M$ of length m-bytes.
**OUTPUT**: MIC $(L, R)$ of 4-bytes each.
1.$K$ is separated into two 4-byte values $k_0, k_1$
  Initialize: L, R
  $L \leftarrow k_0$ and $R \leftarrow k_1$
2. Pad the message $M$ with 1-byte 0x5a and with 0's until the length becomes a 4 multiple.
3.
for $i = 0$ to $n - 1$ do
  $L \leftarrow L\ xor\ m(i)$
  $R \leftarrow R\ xor\ (L << 17)$
  $L \leftarrow (L + R)\ mod\ 2^{32}$
  $R \leftarrow R\ xor\ swap(L)$
  $swap$ is defined as $swap(xyzc) \leftarrow yxcz$ where x,y,z,c are bytes
  $L \leftarrow (L + R)\ mod\ 2^{32}$
  $R \leftarrow R\ xor\ (L << 3)$
  $L \leftarrow (L + R)\ mod\ 2^{32}$
  $R \leftarrow R\ xor\ (L >> 2)$
  $L \leftarrow (L + R)\ mod\ 2^{32}$
end for
```

TABLE I: Comparison of the RC-4T and the WPA algorithms

Criteria	**RC-4T**	**WPA**
Secret key size	32- bits	128- bits
Encryption algorithm	*Toeplitz*, RC-4	TKIP, RC-4
IV length	24-bits	48-bits
Data integrity Algorithm	CRC-32	Message Integrity Code (MIC)
Replay Attacks	No protection	IV sequence
Forgery	No protection	MIC

FPGA. Also, the resources are compared for the aforementioned algorithms in terms of hardware complexity and performance.

A. FPGA implementation of WPA and RC-4T algorithms

A VHDL model for WPA has been developed and the same has been prototyped using *Xilinx Virtex-6q* FPGA device. The encryption and decryption stages are pooled together into a single module.

The FPGA prototyping of the proposed RC-4T model has also been carried out using *Xilinx Virtex-6q* device and ISE Design Suite-14.7. A VHDL model of Algorithm 2 for the RC-4T has been developed. Another VHDL model for RC-4T has also been developed and synthesized excluding the *Toeplitz* stage, which transforms into WEP in order to analyse the hardware complexities.

Algorithm 2 RC-4T encryption algorithm

```
**INPUT** : Message $M$ of length $m$ $bytes$.
**OUTPUT**: Cipher $C$ of length $m + 4$ $bytes$.
1. Choose an $IV$ of length 3 bytes randomly.
  $IV \leftarrow random()$
2. Let S is the secret key generated from Toeplitz hash function.
  $S \leftarrow Toeplitz()$
3. Concatenate the IV with the secret key S.
  $S \leftarrow S$ & $IV$
4. S is used in RC-4 algorithm to generate the key stream.
5. Key Scheduling Algorithm (step-1 in RC-4).
Let L and S-box SB be vectors of length 256 bytes.
for $i = 0$ to 255 do
  $L(i) \leftarrow S(i\%k)$ {k is length of S after concatenation}
end for
Initializing the S-box: $SB(0 : 255) \leftarrow 0, 1, 2, .....255$ and $j \leftarrow 0$
for $i = 0$ to 255 do
  $j \leftarrow (j + L(i) + SB(i))$ % 256
  $SB(i) \leftrightarrow SB(j)$
end for
6. Pseudo Random Generation Algorithm (Step-2 in RC-4)
$i \leftarrow 0$ and $j \leftarrow 0$
while true do
  $i \leftarrow (i + 1)$ % 256
  $j \leftarrow (j + SB(i))$ % 256
  $SB(i) \leftrightarrow SB(j)$
  $t \leftarrow (SB(i) + SB(j))$ % 256
  $K \leftarrow SB(t)$
end while
7. Compute the value of ICV and concatenate with message.
  $ICV \leftarrow CRC(M)$ {ICV length is 4 bytes}
  $M \leftarrow M$ & $ICV$
8. Obtain the encrypted message by XORing the message with key stream from RC-4.
  $C \leftarrow M\ xor\ K$ {K is continuosly generated}
```

Algorithm 3 presents the *Toeplitz* hash function used in the RC-4T encryption.

Algorithm 3 *Toeplitz* Hash Generation Algorithm

```
**INPUT** : Public Key $P$ of length 4 bytes.
**OUTPUT**: Hash $H$ of length 4 bytes.
1. Initialize the seed value
$seed \leftarrow random()$ {4 byte value}
2. Let $V$ is the coefficient vector derived from the irreducible polynomial.
3. State vector T is generated using LFSR approach
$T(94 : 63) \leftarrow seed$ ;   $T(62 : 0) \leftarrow 0$
for $i = 62$ to 0 do
  for $j = 31$ to 0 do
    $T(i) \leftarrow (V(j)\ and\ T(i + j + 1))$ xor $T(i)$;
  end for
end for
4. Hash computation
Initialize: $H \leftarrow 0$
for $i = 31$ to 0 do
  for $j = 63$ to 0 do
    $H(i) \leftarrow (T(31 + j - i)$ and $P(j))$ xor $H(i)$;
  end for
end for
```

TABLE II: Comparison of Synthesis Results of the RC-4T and WPA algorithms in VHDL

Device Utilisation Summary	**RC-4T**	**WPA**
Number of Slice LUTs	65435	81246
Number of fully used LUT-FF pairs	0	0
Number of bonded IOBs	160	96
Macro Statistics		
Adders/Subtractors	69	101
Multiplexers	8112	8112
XORs	68	105
Timing Summary		
Maximum Combinational path delay	5.624 ns	0.837ns

V. Results and simulation

Both the algorithms WPA and RC-4T have been synthesized using *Xilinx* ISE Design Suite-14.7. The simulation results of the RC-4T algorithm considering pair of arbitrary values of inputs and public-keys is given in Figure 3. RC-4T model has also been synthesized without considering the *Toeplitz* hash function. The model uses 69,858 slice LUTs without *Toeplitz*, which proves that the implementation of *Toeplitz* hash function does not consume much hardware when compared to the entire model. Hence the WEP may be replaced with the dynamic model RC-4T using the same hardware.

The WPA algorithm has also been synthesized and simulated in the same way as in RC-4T. Figure 4 provides the simulation results for the WPA. Table II provides a comparison of the synthesis results of both the algorithms. Theoretically, TKIP algorithm involves more arithmetic operations compared to the *Toeplitz* hash generation algorithm. WPA includes the computation of MIC to avoid forgery, which is absent in RC-4T. The aforementioned

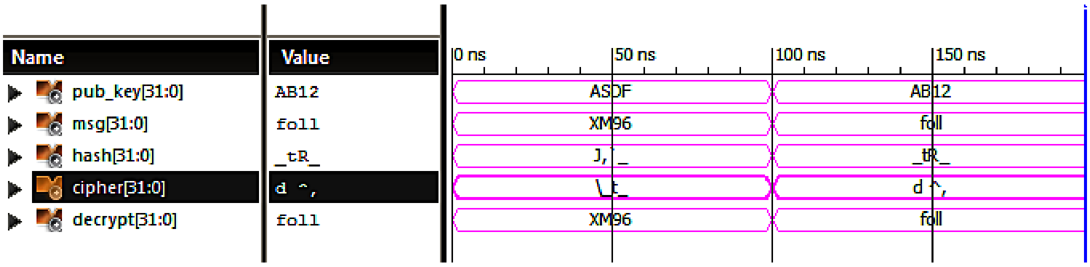

Fig. 3: Simulation Result of RC-4T algorithm on FPGA

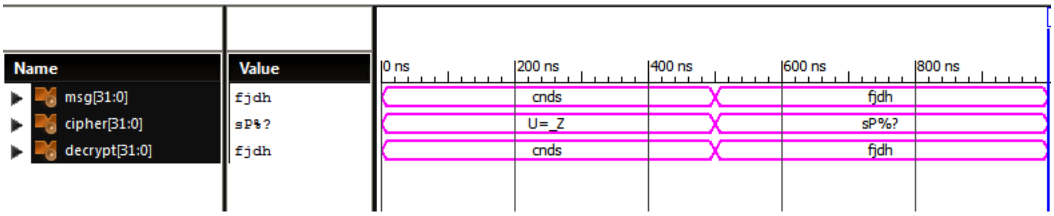

Fig. 4: Simulation Result of WPA algorithm on FPGA

incentives theoretically prove that WPA consumes more hardware. The slice LUTs consumed by WPA is $81,246$, whereas $65,435$ LUTs have been consumed by RC-4T, which justifies the analysis. The combinational delay of WPA is 0.837 ns which is very less compared to that of RC-4T which is 5.624 ns.

VI. Conclusion

In this work the implementations of the proposed algorithm, RC-4T and the WPA algorithm have been carried out using *Xilinx Virtex-6q*FPGA device. The synthesis results of both the implementations indicate that WEP can be replaced by the proposed dynamic stream cipher RC-4T using the same hardware. The proposed algorithm avoids the cryptanalytic methods to decrypt the data by using the dynamic key that is obtained from the variable public key. Based on the comparison of the synthesis results of both RC-4T and WPA, it may be concluded that RC-4T is better than WPA for resource constrained applications such as wireless sensor networks. In case the application requires a faster execution, the WPA may be chosen. WPA has an advantage of the least number of attacks.

References

[1] N. Gupta and G. Biswas, “Wep implementation using linear feedback shift register (lfsr) and dynamic key,” in *Computer and Communication Technology (ICCCT), 2011 2nd International Conference on*, Sept 2011, pp. 422–427.

[2] A. Lashkari, M. Danesh, and B. Samadi, “A survey on wireless security protocols (wep, wpa and wpa2/802.11i),” in *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, Aug 2009, pp. 48–52.

[3] A. Lashkari, M. Mansoor, and A. Danesh, “Wired equivalent privacy (wep) versus wi-fi protected access (wpa),” in *2009 International Conference on Signal Processing Systems*, May 2009, pp. 445–449.

[4] E. Tews, R.-P. Weinmann, and A. Pyshkin, “Breaking 104 bit wep in less than 60 seconds,” in *Information Security Applications.* Springer, 2007, pp. 188–202.

[5] H. Boland and H. Mousavi, “Security issues of the ieee 802.11b wireless lan,” in *Electrical and Computer Engineering, 2004. Canadian Conference on*, vol. 1, May 2004, pp. 333–336 Vol.1.

[6] Y. Wang, Z. Jin, and X. Zhao, “Practical defense against wep and wpa-psk attack for wlan,” in *Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on*, Sept 2010, pp. 1–4.

[7] G. Gounaris, “Wifi security and testbed implementation for wep/wpa cracking demonstration,” 2014.

[8] H. I. Bulbul, I. Batmaz, and M. Ozel, “Wireless network security: Comparison of wep (wired equivalent privacy) mechanism, wpa (wi-fi protected access) and rsn (robust security network) security protocols,” in *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop.* ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, p. 9.

[9] A. Gin and R. Hunt, “Performance analysis of evolving wireless ieee 802.11 security architectures,” in *Proceedings of the International Conference on Mobile Technology, Applications, and Systems.* ACM, 2008, p. 101.

[10] P. Deepthi and P. Sathidevi, “Design, implementation and analysis of hardware efficient stream ciphers using lfsr based hash functions,” *Computers & Security*, vol. 28, no. 3, pp. 229–241, 2009.

[11] P. Rizomiliotis, “Misusing universal hash functions: security analysis of a hardware efficient stream cipher model using lfsr based hash function,” in *Information Theory Workshop (ITW), 2010 IEEE*, Jan 2010, pp. 1–5.

[12] T. Beyrouthy, A. Razafindraibe, L. Fesquet, M. Renaudin, S. Chaudhuri, S. Guilley, J.-L. Danger, and P. Hoogvorst, “A novel asynchronous e-fpga architecture for security applications,” in *Field-Programmable Technology, 2007. ICFPT 2007. International Conference on*, Dec 2007, pp. 369–372.

[13] N. Sklavos, G. Selimis, and O. Koufopavlou, “Fpga implementation cost and performance evaluation of ieee 802.11 protocol encryption security schemes,” in *Journal of Physics: Conference Series*, vol. 10, no. 1. IOP Publishing, 2005, p. 361.