SLDEB: Design of a Secure and Lightweight Dynamic Encryption Bio-Inspired Model for IoT Networks

Bhavesh Kataria, Harikrishna B. Jethva, Pushpmala Vijay Shinde, Satish S. Banait, Farhadeeba Shaikh, Samir Ajani

1 Department of Information Technology, LDRP Institute of Technology and Research, Kadi Sarva Vishwavidyalaya established by SVKM, Gandhinagar 382016, Gujarat, India
2 Department of Computer Engineering, Government Engineering College, Patan 384265, Gujarat, India
3 School of Computer Engineering and Technology, MIT-AOE, Alandi, Pune 412105, Maharashtra, India
4 K.K.Wagh Institute of Engineering Education and Research, Nashik, SPPU Pune 422003, Maharashtra, India
5 MIT WPU School of Polytechnic and Skill Development, Pune 411048, Maharashtra, India
6 Department of Computer Science & Engineering (Data Science), St. Vincent Pallotti College of Engineering and Technology, Nagpur 441108, Maharashtra, India

Corresponding Author Email: bhavesh.iisc@gmail.com

(This article is part of the Special Issue Technology Innovations and AI Technology in Healthcare)

https://doi.org/10.18280/ijisse.130214

Received: 20 February 2023
Accepted: 14 March 2023

Keywords:
IoT, encryption, lightweight, delay, decryption, complexity, energy, security, context, elliptic, cryptic

ABSTRACT
Designing encryption models for IoT deployments requires analysis of multiple network level constraints. These include, estimation of energy requirements, security strength, encryption & decryption delay, computational complexity, etc. A wide variety of models are proposed to perform these tasks, but most of them are either highly complex, or require higher energy levels for encrypting data samples. Moreover, these models are context-independent, and cannot be used for application-specific deployments. To overcome these issues, this text proposes design of a novel secure and lightweight dynamic encryption bioinspired model for IoT networks. The proposed model initially uses an Elliptic Curve Cryptography (ECC) process for data security, and optimizes its performance via Bacterial Foraging Optimization (BFO). ECC parameters that are obtained via BFO are further fine-tuned using a Q-Learning based process, which assists in identification of context-specific parametric ranges for different network types. The combination of BFO with Q-Learning results in dynamic ECC curves, which can be used for context-specific deployments. Performance of the model was evaluated on different scaled networks, and compared with other state-of-the-art encryption models in terms of encryption delay, decryption delay, security level under different attacks, and energy consumption levels. Based on this comparison, it was observed that the proposed model showcased 8.5% lower encryption delay, 3.2% lower decryption delay, and 5.9% lower energy consumption while maintaining similar security levels. Due to these enhancements, the proposed model is useful for a wide variety of low complexity IoT deployments.

1. INTRODUCTION
As a result of advances in technology, Internet of Things (IoT) devices that are linked together are becoming increasingly widespread. Maintaining everyone's safety is the first and most important priority. When compared to the security of Internet of Things devices, the safety of transportation networks is on par, if not higher, on the priority scale [1]. Asymmetrical cryptosystems have been around since 1986, when Miller [2] and Koblitz [3] originally developed the concept of elliptic curve cryptography (ECC), which stands for elliptic curve cryptography. There are several organizations around the globe that have given ECC its stamp of approval, including NIST [4], ANSI [5], and IEEE [6]. There have been a few different proposals for ECC hardware implementations [7]. Two of these approaches are the multiplier and the adder, and they are used in the process of putting modular multiplication into action (MM). Using the Montgomery multiplication technique is another example of multiplier-based architecture [8]. Another example is designing for a certain prime field. Interleaved multiplication is used to construct this adder-based design [9], which was described before. The central processing unit employs a Montgomery MM algorithm that has a multiplier that is r bits by r bits [10]. A multiplier that is n bits by n bits is used in the construction of the processors [11]. MM is a mathematical operation that incorporates both multiplication and quick reduction over a given prime field. It is essential to take into consideration the fact that the design based on multipliers calls for a substantial number of physical resources.

Efficient cipher chaining (ECC) also makes use of modular inversion, which is a process that takes a significant amount of time (MI). One example of this is the implementation of algorithms for binary modular inversion in hardware-efficient computers. The MM and MI units of the processor's 11-bit adder function independently from one another. The IMM
approach is used by processors in order to do radix-4 booth encoding [12]. A radix-2 MM algorithm is used by the processor Durga et al. [13], Huang [14] in order to successfully complete MM while avoiding MI with projective coordinates. The software that is used for traditional cryptography algorithms has drawbacks, such as a high-power consumption and a lengthy processing time; nevertheless, these problems might be resolved with computational advancements. An ECC is similar to RSA in that it is a public-key cryptosystem, but because to developments in computers, it may be easier to use. The primary distinction between it and RSA is that it has the ability to evolve more quickly.

Similarly work in Huang [15], Wei et al. [16], Abd El-Latif et al. [17], Li et al. [18], Mamvong et al. [19], Niu et al. [20], which propose use of multiple authority attribute-based encryption, blockchain based data access control ABE (DAC ABE), controlled alternate quantum walks (CAQWs), Decisional Bilinear Diffie-Hellman (DBDH), power efficient encryption, and key aggregation searchable encryption (KASE), which assist in improving performance of encryption under different use cases. Extensions to these models are discussed in Fotovvat et al. [21], Fotovvat et al. [22], Khan et al. [23], Hussain et al. [24], Khashan [25] which propose use of Lightweight cryptography (LWC), Key-Policy Attribute Based Encryption (KPABE), Secure Surveillance Mechanism, Certificate Based Signcryption with Proxy Re-Encryption (CBSRE), and Lightweight Proxy Re-Encryption, which assists in improving security performance for different use cases. These models must be validated for large-scale networks, and can be extended via use of Compressive-Sensing-Based Lightweight Encryption [26-28], Ciphertext-Policy Hierarchical Attribute-Based Encryption [29], which aim at incorporating lightweight encryption models for IoT network scenarios. This presents those who research cryptographic algorithms with a fresh and fascinating path of exploration to pursue. It is possible to use ECC keys that are smaller and yet provide the same degree of security as RSA. The security provided by ECC, which has 163 bits rather than RSA’s 1024 bits, may be considered an alternative. In addition, electronic communications work especially well as a complement to wireless media such as smart cards and mobile phones, which helps to make ECC a perfect wireless communication protocol. It has been shown that the EC point multiplication algorithm is more time and resource efficient than the RSA exponentiation algorithm. Function of Normal Distribution Extracted from an Algorithm the Elliptic Curve Cryptography (ECC) standard incorporates key exchange, agreement protocols, digital signature (ECDSA), as well as other applicable asymmetric cryptographic primitives. The operation of point multiplication, which is the foundation of all ECC primitives, is also the operation that requires the highest amount of computational work to complete. When it comes to encrypting data samples, it was discovered that the vast majority of models are either too complicated or waste an excessive amount of energy. This is despite the fact that various models have been developed to do these activities. These models are not suitable for usage in app-specific deployments since they are not sensitive to the surrounding environment. Bhattacharya and Pandey [30], Bhattacharya and Pandey [31], Wang and Liu [32], Noura et al. [33], Deb et al. [34], Zhuang et al. [35], Al-Moliki et al. [36] discuss various issues and challenges related to incorporating the Internet of Things (IoT) and green technology, as well as different encryption methods and technologies for securing IoT devices and networks. They propose solutions such as “CEaaS: Constrained Encryption as a Service in Fog-Enabled IoT” and “A Single-Pass and One-Round Message Authentication Encryption for Limited IoT Devices” to enhance security in IoT. They also propose a “Verifiable Searchable Encryption Framework Against Insider Keyword-Guessing Attack in Cloud Storage” to improve the security of cloud storage [37].

In the next section of this article, we will provide our answer to these problems, which is the creation of an innovative, bio-inspired dynamic encryption model that is both lightweight and secure for use in IoT networks. As a result, the objective of this article is to include bioinspired processes in order to offer security assurance for Internet of Things devices in a way that is as simple and uncomplicated for different use cases.

2. PROPOSED SECURE AND LIGHTWEIGHT DYNAMIC ENCRYPTION BIOINSPIRED MODEL FOR IOT NETWORKS

Based on the review of existing encryption models, it can be observed that most of these models are either highly complex, or require higher energy levels for encrypting data samples. Moreover, these models are context-independent, and cannot be used for application-specific deployments. To overcome these issues, this section proposes design of a novel secure and lightweight dynamic encryption bioinspired model for IoT networks. Flow of the model is depicted in Figure 1, where it can be observed that the proposed model initially uses an Elliptic Curve Cryptography (ECC) process for data security, and optimizes its performance via Bacterial Foraging Optimization (BFO). ECC parameters that are obtained via BFO are further fine-tuned using a Q-Learning based process, which assists in identification of context-specific parametric ranges for different network types. The combination of BFO with Q-Learning results in dynamic ECC curves, that can be used for context-specific deployments.

![Figure 1](image-url) Overall flow of the proposed light-weight encryption process
The model initially collects information about different ECC curves, that include but are not limited to ANSSI FRP256v1, BN (2, 254), Curve1174, Curve383187, E-382, M-383, NIST P-224, secp256k1, etc. These curves have their own varying prime fields, binary fields, and Koblitz fields.

For instance, the Curve1174 is represented via Eq. (1):

$$x^2 + y^2 = 1 - 1174x^2y^2$$ (1)

Which can be represented via Figure 2(a), where a quad parabolic shape can be observed for different x & y sample sets. Similarly, the secp256k1 curve, which is used by Bitcoin for block-level encryptions can be evaluated via Eq. (2), and is depicted in Figure 2(b), as follows:

$$y^2 = x^3 + 7$$ (2)

Based on these curve sets, it can be observed that for every value of x, the curve has 2 similar points on the Y axis. One of these points are used for encryption, while other is used for decryption process. The proposed model uses this characteristic of ECC in order to generate light-weight curves via BFO model, which works as per the following process.

- Initialize optimization parameters of BFO as follows:
  - Total number of bacteria particles used during optimization ($N_p$);
  - Total optimization iterations for BFO ($N_i$);
  - Chemotaxis rate ($L_r$);
  - Rate at which particles regenerate ($L_e$);
  - Rate of elimination ($L_d$);
  - Total available ECC curves and their parameters ($N_c$).

- Initially generate bacterial swarm as per the following process:
  - Select a stochastic curve from the set of curves, and estimate its fields as per Eqns. (3), (4), and (5).

$$p = STOCH(L_e \ast p_{max}, p_{max})$$ (3)

$$b = STOCH(L_r \ast b_{max}, b_{max})$$ (4)

$$k = STOCH(L_e \ast k_{max}, k_{max})$$ (5)

where, $STOCH$ represents a Markovian stochastic process, used to generate numbers between given range sets, while $p$, $b$ & $k$ represents prime field values, binary field values, and Koblitz field values for the given curve sets.

- The generated sub-curve is further processed if it follows the rule of ECC, that for every value of $x$, there should be exactly 2 values of $y$, which assists in encryption and decryption processes;

- If the curve doesn’t follow these rules, then it is regenerated via Eqns. (3), (4), and (5) till the conditions are fulfilled for different value sets;

- This new sub-curve is evaluated, and its fitness levels are estimated via Eq. (6):

$$f = \frac{1}{N_i} \sum_{i=1}^{N_i} \frac{d_{ei} + d_{di} + e_{ei} + e_{di}}{d_{ref}}$$ (6)

where, $d_e$ & $d_d$ represents delay needed for encryption & decryption, while $d_{ref}$ represents combined encryption & decryption for the reference curve, while, $e_e$ & $e_d$ represents energy needed for encryption & decryption, while $e_{ref}$ represents combined encryption & decryption energy for the underlying reference curve sets.

- This process is repeated for all particles, and a particle fitness threshold is estimated via Eq. (7):

$$f_{th} = \frac{1}{N_p} \sum_{i=1}^{N_p} \frac{L_e + L_r + L_e}{3 \ast N_p}$$ (7)

- Particles with $f < f_{th}$ are marked as ‘not to be reconfigured’, while others are marked as ‘to be reconfigured’.

  - Once initial configurations are generated, then all particles are scanned for $N_i$ iterations, and the particles marked as ‘to be reconfigured’ are regenerated via Eqns. (3), (4), (5) and (6), which assists in generation of new curve sets.

  - At the end of each iteration, fitness threshold levels are recalculated, and the process is continued for $N_i$ iterations.

At the end of final iteration, select all curves that are marked as ‘not to be reconfigured’, and use a Q-Learning based model to identify optimal curve sets for different IoT use cases. To perform this task, setup target delay $d_t$ and target energy levels $e_t$ that are required by the IoT deployment, and evaluate the
The performance of the individual models used for validation is shown by their labels in the accompanying tables, which tabulate these data. The suggested model’s performance was compared with respect to DAC ABE [16] and CBS RE [23], which helped to validate its performance under various Number of Communication (NC) sequence sets (Table 1).

Table 1. Communication delay with the proposed encryption model averaged over different communication sets

<table>
<thead>
<tr>
<th>NC</th>
<th>Delay (ms)</th>
<th>Delay (ms)</th>
<th>Delay (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DAC ABE [16]</td>
<td>CBS RE [23]</td>
<td>Proposed</td>
</tr>
<tr>
<td>100</td>
<td>0.44</td>
<td>0.50</td>
<td>0.26</td>
</tr>
<tr>
<td>150</td>
<td>0.52</td>
<td>0.60</td>
<td>0.31</td>
</tr>
<tr>
<td>200</td>
<td>0.63</td>
<td>0.72</td>
<td>0.38</td>
</tr>
<tr>
<td>250</td>
<td>0.72</td>
<td>0.83</td>
<td>0.43</td>
</tr>
<tr>
<td>300</td>
<td>0.81</td>
<td>0.93</td>
<td>0.49</td>
</tr>
<tr>
<td>350</td>
<td>0.90</td>
<td>1.04</td>
<td>0.54</td>
</tr>
<tr>
<td>400</td>
<td>1.00</td>
<td>1.14</td>
<td>0.60</td>
</tr>
<tr>
<td>450</td>
<td>1.09</td>
<td>1.24</td>
<td>0.65</td>
</tr>
<tr>
<td>500</td>
<td>1.17</td>
<td>1.34</td>
<td>0.70</td>
</tr>
</tbody>
</table>

Figure 2. Communication delay with the proposed encryption model averaged over different communication sets

Based on this evaluation, and Figure 3, it can be observed that the proposed model showcased 18.5% lower delay when compared with DAC ABE [16], and 25.9% lower delay when compared with CBS RE [23], which makes it useful for high-speed IoT network scenarios. This is due to incorporation of encryption & decryption delays during selection of sub-curve parameters, which assists in improving communication performance under real-time IoT communication sets. Similarly, the energy consumption can be observed from Table 2 as follows:

Table 1. Communication energy levels with the proposed encryption model averaged over different communication sets

<table>
<thead>
<tr>
<th>NC</th>
<th>Energy (mJ)</th>
<th>Energy (mJ)</th>
<th>Energy (mJ)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DAC ABE [16]</td>
<td>CBS RE [23]</td>
<td>Proposed</td>
</tr>
<tr>
<td>100</td>
<td>6.25</td>
<td>7.19</td>
<td>3.73</td>
</tr>
<tr>
<td>150</td>
<td>6.62</td>
<td>7.61</td>
<td>3.95</td>
</tr>
<tr>
<td>200</td>
<td>6.95</td>
<td>8.00</td>
<td>4.15</td>
</tr>
<tr>
<td>250</td>
<td>7.28</td>
<td>8.38</td>
<td>4.35</td>
</tr>
<tr>
<td>300</td>
<td>7.62</td>
<td>8.76</td>
<td>4.55</td>
</tr>
<tr>
<td>350</td>
<td>7.98</td>
<td>9.18</td>
<td>4.76</td>
</tr>
<tr>
<td>400</td>
<td>8.36</td>
<td>9.61</td>
<td>4.99</td>
</tr>
<tr>
<td>450</td>
<td>8.70</td>
<td>10.00</td>
<td>5.20</td>
</tr>
<tr>
<td>500</td>
<td>9.03</td>
<td>10.38</td>
<td>5.39</td>
</tr>
</tbody>
</table>
Based on this assessment and Figure 4, it can be seen that the proposed model demonstrated 28.3% and 34.2% reduced energy usage, respectively, when compared with DAC ABE [16] and R2, which makes it beneficial for high-lifetime IoT network situations. This is because real-time IoT communication sets help to improve communication performance by including encryption & decryption energy levels while choosing sub-curve parameters. Similarly, the throughput of these communications can be observed from Table 3 as follows:

**Table 3. Communication PDR with the proposed encryption model averaged over different communication sets**

<table>
<thead>
<tr>
<th>NC</th>
<th>DAC ABE [16] PDR (%)</th>
<th>CBS RE [23] PDR (%)</th>
<th>Proposed PDR (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>98.92</td>
<td>99.02</td>
<td>98.97</td>
</tr>
<tr>
<td>150</td>
<td>99.05</td>
<td>99.15</td>
<td>99.10</td>
</tr>
<tr>
<td>200</td>
<td>99.17</td>
<td>99.27</td>
<td>99.22</td>
</tr>
<tr>
<td>250</td>
<td>99.27</td>
<td>99.37</td>
<td>99.32</td>
</tr>
<tr>
<td>300</td>
<td>99.36</td>
<td>99.46</td>
<td>99.41</td>
</tr>
<tr>
<td>350</td>
<td>99.47</td>
<td>99.57</td>
<td>99.52</td>
</tr>
<tr>
<td>400</td>
<td>99.59</td>
<td>99.69</td>
<td>99.64</td>
</tr>
<tr>
<td>450</td>
<td>99.71</td>
<td>99.81</td>
<td>99.76</td>
</tr>
<tr>
<td>500</td>
<td>99.83</td>
<td>99.93</td>
<td>99.88</td>
</tr>
</tbody>
</table>

Based on this assessment and Figure 6, it is apparent that the proposed model demonstrated comparable PDR when compared with DAC ABE [16] and CBS RE [23], making it appropriate for real-time IoT network applications. Due to the adoption of high-efficiency encryption methods, which decrease packet losses by mitigating various network threats, the PDR is often high. As a result, the suggested model is extremely effective and can be used for IoT networks with lower complexity and improved energy efficiency and larger data rates, making it scalable for various network situations.

4. CONCLUSION AND FUTURE SCOPE

The proposed model uses a combination of BFO for estimation of initial ECC sub-curves, and optimizes it via continuous Q-Learning operations. The model uses encryption & decryption delay, encryption & decryption energy, and reference curve performance levels in order to identify efficient sub-curve sets. The proposed model therefore demonstrated 18.5% reduced latency in comparison to DAC ABE [16] and 25.9% lower delay in comparison to CBS RE [23], making it effective for high-speed IoT network situations. This is because encryption and decryption delays are taken into account while choosing sub-curve parameters, helping to
improve communication performance for real-time IoT communication sets. It is advantageous for high-lifetime IoT network situations as the proposed model’s energy usage was 28.3% and 34.2% less than that of DAC ABE [16] and [R2, respectively]. This is because real-time IoT communication sets help to improve communication performance by including encryption & decryption energy levels while choosing sub-curve parameters. Secondary measures revealed that the proposed model had 19.5% greater communication throughput compared to DAC ABE [16] and 14.9% higher communication throughput compared to CBS RE [23], making it appropriate for high data-rate IoT network applications. This is because real-time IoT communication sets help to improve communication performance by including processing delay levels and evaluating temporal performance while choosing sub-curve parameters. When compared to DAC ABE [16] and CBS RE [23], the proposed model also showed comparable PDR, which makes it appropriate for real-time IoT network applications. Due to the adoption of high-efficiency encryption methods, which decrease packet losses by mitigating various network threats, the PDR is often high. As a result, the suggested model is very effective and suitable for low-complexity and high energy efficiency applications. Higher data rates on IoT networks make it scalable for many network situations. In future, the model’s performance can be optimized via integration of hybrid bioinspired models that will assist in improving parameter selection for different scenarios. The model must be validated w.r.t. large-scale network sets, and its performance can be further improved via deployment of other encryption techniques which will make it useful for large-scale network scenarios.

REFERENCES


