information

MDPI

Article

A Robust and Hybrid Cryptosystem for Identity Authentication

Ali Takieldeen *, Said H. Abd Elkhalik, Ahmed S. Samra, Mohamed A. Mohamed and Fahmi Khalifa

Electronics and Communications Engineering Department, Faculty of Engineering, Mansoura University, Mansoura 35516, Egypt; sheweda76@gmail.com (S.H.A.E.); shmed@mans.edu.eg (A.S.S.); mazim12@mans.edu.eg (M.A.M.); fahmikhalifa@mans.edu.eg (F.K.)

* Correspondence: a_takieldeen@yahoo.com

Abstract: With the progressive development of a wide range of applications, interconnect things and internet of things (IoT) became an imperative required trend by industries and academicians. IoT became a base infrastructure for remote access or control depending on internet protocol (IP) networks, especially after the COVID-19 pandemic. The huge application domain's infrastructure, which depends on IoT, requires a trusted connection to guarantee security and privacy while transferring data. This paper proposes a hybrid identity authentication pipeline that integrates three schemes, namely, an elliptic curve cryptography (ECC) scheme is integrated with the Ong, Schnorr, and Shamir (OSS) signature scheme and chaotic maps. The latter satisfies both security and guarantee criteria. The novelty of the proposal is in using chaotic mapping and a cyclic group to deduce a substitution box (S-Box) and a reversible matrix as a portion of the OSS signature equation. The ECC-based security part is an efficient public key cryptography mechanism with less computational cost, which makes it the most convenient to be used in IoT devices for authentication and privacy. The strength of the proposed scheme relies on combining the discrete logarithm problem (DLP) and integer factorization problem (IFP). The proposed approach was simulated using Lab-View and compared with other state-of-the art schemes. Extensive simulation results and analysis of the security and time rendering results confirmed its durability against different types of attacks, such as linear and differential attacks.

Keywords: authentication; IoT; differential attack; discrete logarithm problem; elliptic curve cryptosystem; integer factorization; linear attack; OSS signature; reversible matrix

check for updates

Citation: Takieldeen, A.; Abd Elkhalik, S.H.; Samra, A.S.; Mohamed, M.A.; Khalifa, F. A Robust and Hybrid Cryptosystem for Identity Authentication. *Information* **2021**, *12*, 104. https://doi.org/10.3390/info12030104

Academic Editors: Petr Doucek and Antonin Pavlicek

Received: 9 January 2021
Accepted: 6 February 2021
Published: 1 March 2021

1. Introduction

In recent years, remote access technology and device control have become an imperative requirement. Particularly, this is evident nowadays due to the increased spread of the coronavirus pandemic (COVID-19), which necessitated the imposition of some restrictions, including mandatory social distancing in many countries. Therefore, it became clear how developing remote access communication technology is of immense importance depending on the Internet service, especially research in improving the technology of the Internet of things (IoT). The IoT is the technology to assemble devices that need to be monitored, linked, and interacted [1]. IoT is associated with great prospects of physical objects with the cyber world, such as healthcare devices, intelligent transportation systems, home appliances, sensors, and environmental monitoring [2]. Connected devices to the IoT are exponentially increasing [3], which add more security challenges that must be taken into consideration [4]. Cryptosystems based on asymmetric keys play vital roles in the security of diverse communication systems. Cryptanalysis techniques motivate researchers to develop novel signature schemes to dominate the growth in security attacks [5]. The financial field of Bitcoin has become one of the most required research areas for security from cyber-attacks. The blockchain concept succeeded in achieving that, as it provides reliable and secure decentralized solutions [6]. The elliptic curve cryptography (ECC)-based digital signature algorithm (DSA) is used for data signature and verification in wireless devices. Identity-based authentication and access control in wireless network devices help to protect from illegitimate access and preserve the security issues of the wireless nodes [7]. DSA is a robust tool in data authentication and privacy. Since the emergence of public key cryptography in 1970, many schemes have been developed, such as the efficient ECC technique [8]. The cyclic group of order p was also developed, which is isomorphic to the additive group of ((Z/pZ) *,.), where Z is the set of all integers, and p is a prime number.

The ECC algorithm has demonstrated a considerable effectiveness on public key cryptography [9]; as a result, an efficient digital signature approach was proposed in [10]. The strength of the scheme in [10] is its dependence on the discrete logarithm problem (DLP). On the contrary, traditional schemes are challenged by more complicated and effective attacks. This paved the way for the robust security schemes previously represented, while the era of the traditional techniques is expired [11].

To ensure a strong and efficient cryptosystem, it is necessary to achieve Shannon properties, where the permutation process is an important operation. Logistic mapping and cyclic groups are very important steps to ensure the randomness of performance. However, for a robust algorithm that can withstand different attacks, it is important to achieve confusion and diffusion properties [12]. Another goal, in addition to robustness, is to minimize execution time to be applicable in real-time applications. Logistic mapping and cyclic groups are used to generate S-Box, which is important to guarantee the cryptographic strength, such as nonlinearity, bijection, strict avalanche criterion, output bits independence criterion (BIC), and equiprobable input/output XOR distribution [13].

This work proposes a novel signature scheme based on the integration of the ECC algorithm with the Ong–Schnorr–Shamir (OSS) scheme. The robustness of the proposed approach relies on using a reversible key matrix of 4×4 as a portion of the OSS signature equation with decoding modification on ECC algorithm. This consolidation increases the degree of complexity and thus increases the confidentiality of the data. To prove the novelty and credibility of the presented technique, the new scheme was tested and demonstrated robustness against other approaches.

The rest of this manuscript is sequenced as follows. Section 2 introduces the previous work related to the proposed pipeline. Section 3 details the proposed methodology and the employed schemes (i.e., the ECC and the OSS signature schemes). Section 4 outlines the details of the proposed OSS–ECC digital signature technique. Robustness measures of the proposed scheme are demonstrated and discussed in Section 5, and conclusions are given is Section 6.

2. Related Work

Many institutions, including the US government, rely on elliptic curve (EC) technology to encrypt their data, as it is a multi-factor robust authentication and encryption technique [14]. Khatoon et al. [15] proposed an efficient and secure, bilinear pairing-based mutual authentication and key agreement protocol based on elliptic curve cryptography hardness for healthcare applications. Nikooghadam and Amintoosi [16] demonstrated the weaknesses of the protocol in [15], as it is vulnerable to known session-specific temporary information attack and is not able to provide perfect forward secrecy. Rahim et al. [17] applied the Ong–Schnorr–Shamir (OSS) subliminal channel scheme in securing data communication, which is a cryptographic method and supports verification based on the OSS digital signature scheme. Depending on OSS, as the basic signature algorithm is no longer possible, Pollard and Schnorr [18] presented an efficacious solution to solve the quadratic equation $x^2 + ky^2 = m \bmod n$. Their technique succeeded in obtaining the signature without any knowledge about the private key. This would be a critical point if we decided to depend on the OSS scheme for authentication. So, the authentication scheme proposed in [18] has shown more robustness and reliability in data security than in previous works.

Recently, Biswas [19] introduced an alternative approach to realize better privacy and lower decentralized identifiers by implementing ring signatures for anonymous authentication. Their approach was implemented based on an android phone with real data, and the signature was designed using the combination of Curve25519 and SHA-512 hashing algorithms. The generation and verification consumed time was 0.875 and 1.06 msec, respectively. An authentication model, called the tree of trust (VTT), for use in IoT was presented by Shingala [20]. The VTT aimed to provide embedded device-friendly entity authentication and limit the trust peripheries. Based on an embedded platform, the public key identifier was evaluated based on the ability of the elliptic curve digital signature algorithm (ECDSA) to verify and SHA-256 digest operations. Chen et al. [21] proposed an authentication scheme applying authenticating identity-based cryptography to protect an entire system from the compromised machine-to-machine service provider (MSP). In their scheme, partial secrets are stored in MSP to prevent it from endangering the whole system.

3. Methodology

The proposed security scheme is based on the integration of (i) the ECC algorithm, (ii) chaotic maps, and (iii) the OSS digital signature algorithm. An overview of the main components of the proposed system is given in the following subsections.

3.1. Elliptic Curve Cryptosystem (ECC)

The elliptic curve cryptosystem, or ECC, provides most of the significant features when compared with other public key algorithms [22]. With fewer mathematics, small key length, and less storage space, the ECC presents an adequate level of data security. This has led researchers to consider ECC as a lightweight authentication scheme in many IoT applications [23–25]. Currently, it is the security backbone for many applications and systems, such as mobile devices and network protocols [26,27]. Mathematically, the ECC can be defined using the Weierstrass equation as:

$$y^2 \equiv x^3 + ax + b \bmod p \tag{1}$$

where $(x, y) \in Z_p$ is the set of all integers; p is a prime number >3; and a and $b \in Zp$ are subject to

$$4a^3 + 27b^2 \neq 0 \bmod p \tag{2}$$

The EC group, or $E(Z_p)$, contains all points satisfying Equation (1) and the point at the infinity O [28]. In the literature, there are many curves introduced for ECC; see Figure 1.

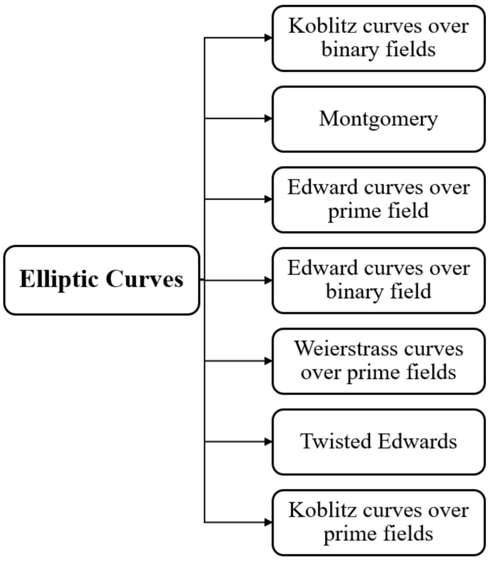

Elliptic Curves
Koblitz curves over binary fields
Montgomery
Edward curves over prime field
Edward curves over binary field
Weierstrass curves over prime fields
Twisted Edwards
Koblitz curves over prime fields

Figure 1. Illustration of special elliptic curve types, adopted from [29].

There are two fundamental mathematical point operations for the ECC algorithm: addition and multiplication. Scalar multiplication consists of point summation and doubling [30]. Figure 2 shows both operations. As demonstrated in the figure, two points are used, $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, and the summation point R = (x_3, y_3) can be estimated in two different scenarios:

(1) If $P > Q$: R = $P + Q$, which can be calculated by drawing a line passing through P and Q, then R is the mirror point of the third intersection point (R′), as shown in Figure 2a.

(2) If $P = Q$: R = $2Q$, which can be estimated by drawing a tangent line through Q, then the doubling point R is the mirror point of the second intersection point, as clarified in Figure 2b. where

$$x_3 = \mu^2 - x_1 - x_2 \bmod p \tag{3}$$

$$y_3 = \mu\,(x_1 - x_3) - y_1 \bmod p \tag{4}$$

and

$$\mu = \frac{3{x_1}^2 + a}{2\,y_1} \bmod p \text{ if } p \; = \; Q \tag{5}$$

$$\mu = \frac{y_{2-}\,y_1}{x_{2-}\,x_1} \bmod p \text{ if } p \; \neq \; Q \tag{6}$$

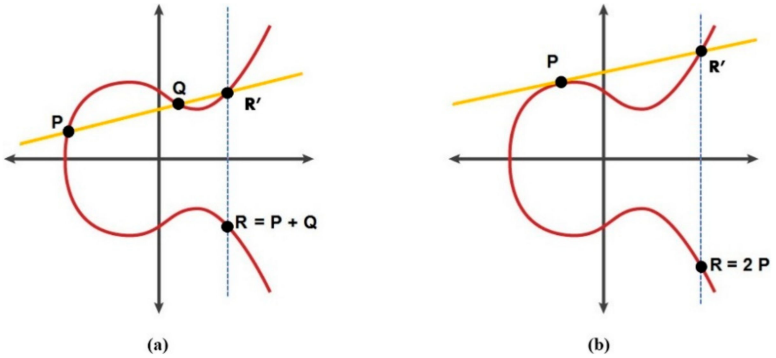


Figure 2. Demonstration of elliptic curve mathematical operations: (**a**) point summation and (**b**) point doubling.

ECC computations depend on the nature that they are defined for, which can be finite field operations, EC group operations, or curve operations. Figure 3 shows the differences between these computations.

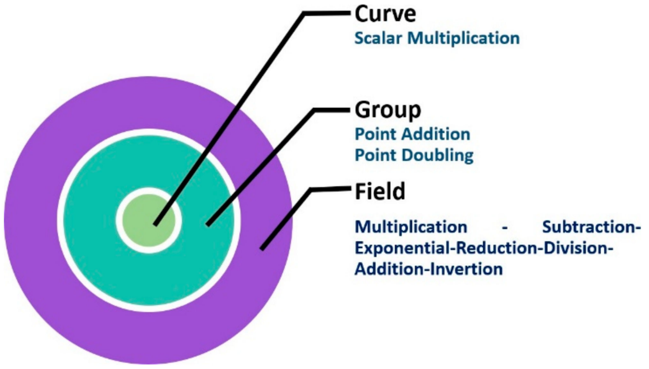


Figure 3. Illustration of elliptic curve cryptography operations.

3.2. *OSS Signature Scheme*

Rapidity and guarantee are prime features in any authorized signature scheme. Any technique that satisfies those two features will be realizable and effective in many fields. Ong, Schnorr, and Shamir designed an effective scheme that is based on a functional quadratic equation [31]. Their scheme has an importance advantage of providing speedy signature generation and verification, while requiring only a single inversion and two modular multiplications. However, three multiplications are needed for validation.

The robustness of the OSS is in its underlying mathematical equation: $x^2 + ky^2 = m$ mod n, which is hard to solve. Here, m represents the original message, k is the public key, and n is derived from Euler's theorem [32]. Figure 4 illustrates the OSS scheme's flowchart. The receiver (interrogator) checks correctness of the previous formula using the received pair (x, y) generated at the receiver. The computation of $w^{-1}(\text{mod } n)$ and $k = w^2(\text{mod } n)$, where k, n, and w are the public key and w^{-1} is the private key, is illustrated at Figure 4.

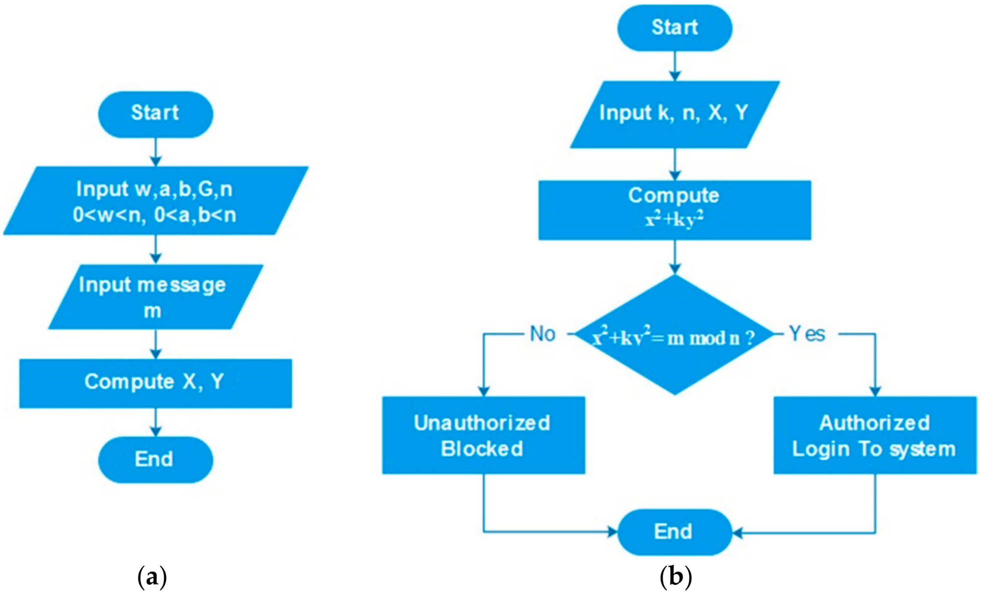


Figure 4. Traditional Ong–Schnorr–Shamir (OSS) signature scheme: (**a**) transponder and (**b**) interrogator flowcharts.

3.3. Logistic Map and Cyclic Group

The third scheme that is utilized in our system is chaotic maps. Chaotic systems are strong tools to select random numbers. They have desirable features, such as ergodicity, complex structural, high randomness, and mixing, according to the following equation:

$$x(n+1) = \lambda x(n)(1 - x(n)) \tag{7}$$

where $x(n)$ is the initial condition, and λ is the system parameter that is used as a key [33]. The above map is chaotic when $3.9 < \lambda < 4.0$.

If every element in a given group (G) can be represented as a power α^r (r is integer) of a fixed element $\alpha \in G$, then G is said to be a cyclic group. Here, α is known as the generator of group, which can be finite or infinite [34]: α^r modulo p; here, $r \in [1,\ p-1]$ and p is a prime number. By considering $p = 17$, each number in {3, 5, 6, 7,10, 11, 12, 14} is said to be a generator.

According to the cyclic group theory, it can be noticed that the prime number 257 has 128 generators, and we can choose between them. A chaotic equation is used to choose randomly between the 128 generators, and the seed number for this chaotic equation is considered as the key. Table 1 contains the 128 generators of 257.

Table 1. The generator list of the prime number 257.

3	5	6	7	10	12	14	19	20	24	27
28	33	37	38	39	40	41	43	45	47	48
51	53	54	55	56	63	65	66	69	71	74
75	76	77	78	80	82	83	85	86	87	90
91	93	94	96	97	101	102	103	105	106	107
108	125	109	110	112	115	119	126	127	130	131
132	138	142	145	147	148	149	150	151	152	154
155	156	160	161	163	164	166	167	170	171	172
174	175	177	179	180	181	182	183	186	188	191
192	194	201	202	203	204	206	209	210	212	214
216	217	218	219	220	224	229	230	233	237	238
243	245	247	250	251	252	254				

4. The Proposed Oss–ECC Digital Signature

Figure 5 presents the flowchart of the proposed data signature. The interrogator sends data to the transponder, which are the S-Box output with EC parameters and the public key. The transponder receives the data and performs inverse S-Box to obtain the message "m" and uses the public key and EC parameters to calculate "t". Using t and m, the transponder generates the signature x, y and sends it to the interrogator, which verifies the signature of the transponder and produces m. As mentioned above, the proposed pipeline utilizes three hybrid authentication schemes: the ECC algorithm, chaotic maps, and the OSS digital signature algorithm. The robustness of the proposed technique depends on the hardness of the ECDLP and the modifications using chaotic mapping and cyclic groups. The integration of those three schemes is intended to increase the privacy and makes it more efficient than traditional authentication schemes. Additionally, the signature generation became faster than before and the inverse of the key matrix became unnecessary.

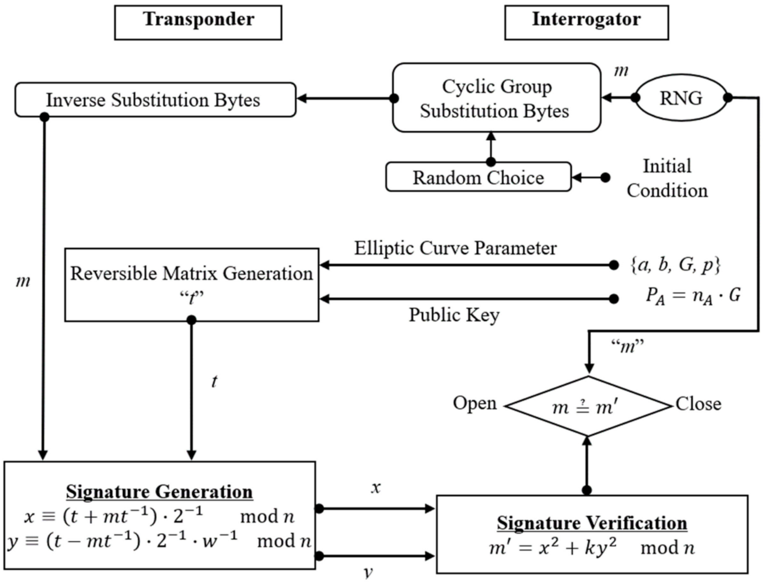


Figure 5. The proposed OSS digital signature flowchart based on elliptic curve cryptography (ECC).

4.1. Substitution-Box (S-Box) Construction

Substitution-Box (S-Box) is an important concern in constructing any secure cryptosystem. S-Boxes are used to provide diffusion and confusion [35]. Various work has been proposed in the literature. For example, Ruming et al. [36] proposed an S-box that depended on the iteration of continuous chaotic maps. Their key-dependent S-box was constructed with the logistic map. Guo et al. [37] presented an extended method for designing S-Box based on three-dimensional chaotic Baker maps. This depends on obtaining strong 8 × 8 S-boxes. Three-dimensional chaotic Baker maps present an intensive chaotic character in addition to resist several attacks. In this paper, an 8-bit input/output S-box was constructed based on the cyclic group. Unlike previous work, it is a 16 × 16 S-box. Table 1 presents all possible generators for prime number 257, which was used to construct the required S-Box based on Equation (8) of the 2D logistic equation.

4.2. Random Choice

In this process, one random generator (RNG, α) is chosen from Table 1, which is used to construct the required S-Box, by using the 2D logistic equation to select the random generator as follows:

$$x\ (n+1) = [\lambda x(n)\ (1 - x(n))\ \text{Modulo } 128] + 1 \tag{8}$$

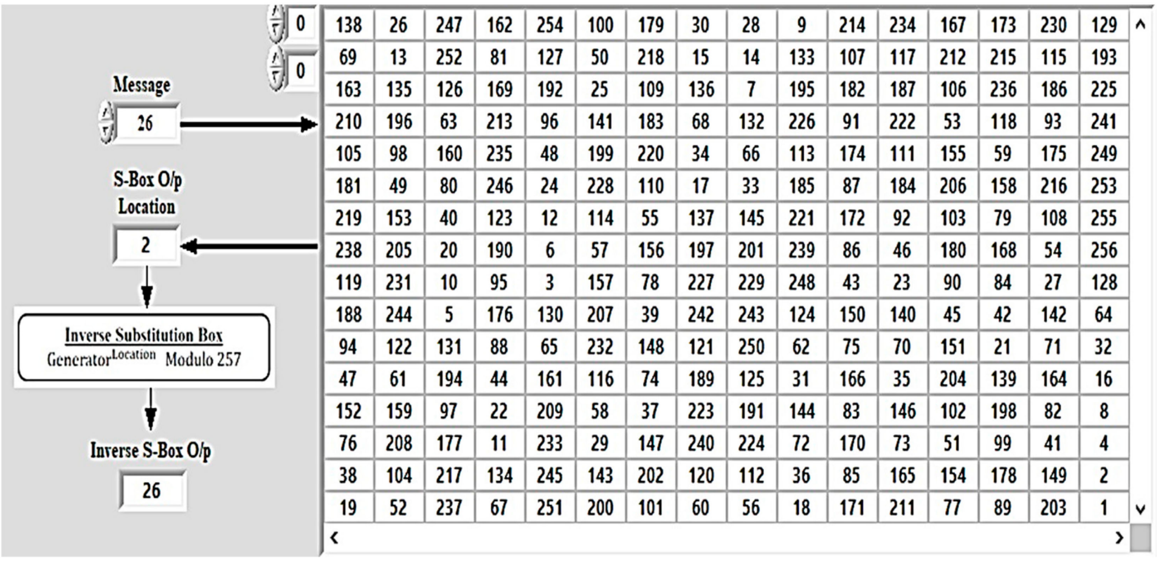
where $x(n)$ is the initial (integer number) condition, and λ is the system parameter, which works as the secret key. The map is chaotic for $3.9 < \lambda < 4.0$, which is used as a key. The S-Box of each round is computed by calculating the cyclic group of the generator using:

$$\alpha^{r}\ \text{modulo } 257 \tag{9}$$

where $r \in [1,\ 256]$. The substitution process is based on replacing the 8-bit input with the "location of the similar 8 bits from the cyclic group-1". The inverse of the substitution process relies on computing:

$$\alpha^{((8\ \text{bits})\text{input}+1)}\ \text{modulo } 257 \tag{10}$$

The resulted data output is the same as the original data input. Figure 6 presents the cyclic group outputs with length 256. This process is simulated using Lab-View, and the results are organized as shown.



0
0

Message
26

S-Box O/p
Location
2

Inverse Substitution Box
$\text{Generator}^{\text{Location}}$ Modulo 257

Inverse S-Box O/p
26

138	26	247	162	254	100	179	30	28	9	214	234	167	173	230	129
69	13	252	81	127	50	218	15	14	133	107	117	212	215	115	193
163	135	126	169	192	25	109	136	7	195	182	187	106	236	186	225
210	196	63	213	96	141	183	68	132	226	91	222	53	118	93	241
105	98	160	235	48	199	220	34	66	113	174	111	155	59	175	249
181	49	80	246	24	228	110	17	33	185	87	184	206	158	216	253
219	153	40	123	12	114	55	137	145	221	172	92	103	79	108	255
238	205	20	190	6	57	156	197	201	239	86	46	180	168	54	256
119	231	10	95	3	157	78	227	229	248	43	23	90	84	27	128
188	244	5	176	130	207	39	242	243	124	150	140	45	42	142	64
94	122	131	88	65	232	148	121	250	62	75	70	151	21	71	32
47	61	194	44	161	116	74	189	125	31	166	35	204	139	164	16
152	159	97	22	209	58	37	223	191	144	83	146	102	198	82	8
76	208	177	11	233	29	147	240	224	72	170	73	51	99	41	4
38	104	217	134	245	143	202	120	112	36	85	165	154	178	149	2
19	52	237	67	251	200	101	60	56	18	171	211	77	89	203	1

Figure 6. Substitution-box (S-Box) construction using Lab-View.

4.3. Signature Generation and Verification

The interrogator (User A) shares information from the ECDSA with the transponder (User B). Information that is shared is {a, b, G, p}, where a and b are the coefficients of the ECC mentioned in (1), G is the generator basepoint, and p is the prime number equal to $n = [P \times Q]$, which is the Rivest, Shamir, and Adleman (RSA) moduli. Both interrogator and transponder select their private key {$\mathrm{n_A}$, $\mathrm{n_B}$} randomly from the interval $[1, p - 1]$. Equation (11) shows the generation of the interrogator's public key.

$$P_A = n_A \cdot G \tag{11}$$

The transponder uses the interrogator's public key to generate the key pair (*KP)* matrix to generate the initial key $V_I = (x, y)$, by multiplying its private key by the public key of the interrogator.

$$KP = n_B \cdot P_A = n_B \cdot n_A \cdot G = (x, y) \tag{12}$$

where

$$V_1 = x \cdot G = (V_{11}, V_{12}) \tag{13}$$

$$V_2 = y \cdot G = (V_{21}, V_{22}) \tag{14}$$

Now, the transponder (User B) uses the resulted *KP* matrix to generate a reversible matrix "t", where $t = t^{-1}$. Then, the inverse of the *KP* matrix is not needed. The reversible matrix "t" is a 4 × 4 matrix that is generated as follows:

$$t = \begin{bmatrix} V_{11} & V_{12} & V_{13} & V_{14} \\ V_{21} & V_{22} & V_{23} & V_{24} \\ V_{31} & V_{32} & V_{33} & V_{34} \\ V_{41} & V_{42} & V_{43} & V_{44} \end{bmatrix}$$

which can be partitioned as $t = \begin{bmatrix} V_A \, V_B \\ V_C \, V_D \end{bmatrix}$.

The proposed technique considers that V_{A} equals $\begin{bmatrix} V_{11} \, V_{12} \\ V_{21} \, V_{22} \end{bmatrix}$, then the values of the other sections can be calculated by solving $V_B = \mathrm{I} - V_{\mathrm{A}}$, $V_{\mathrm{C}} = I + V_{\mathrm{A}}$, $V_{\mathrm{A}} + V_{\mathrm{D}} = 0$, where I is the identity matrix. Then, the transponder generates the signature by both main equations

$$x \equiv (t + mt^{-1}) \cdot 2^{-1} \bmod n \tag{15}$$

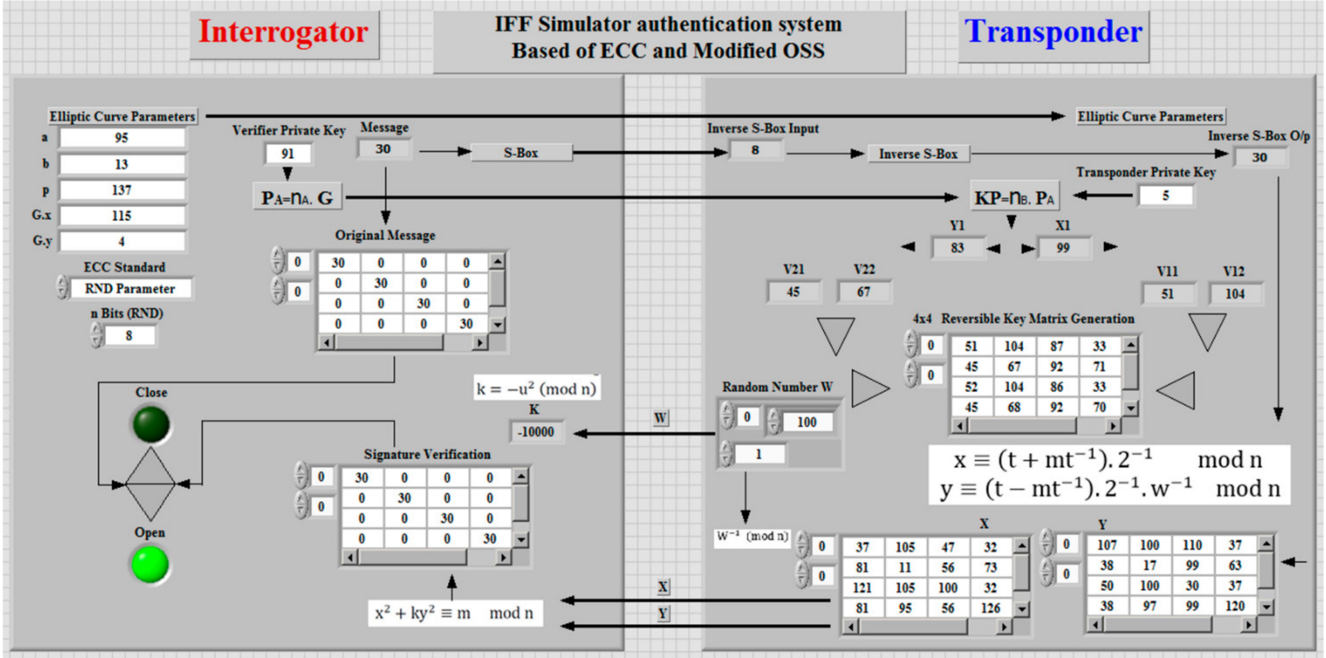
$$x \equiv (t - mt^{-1}) \cdot 2^{-1} w^{-1} \bmod n \tag{16}$$

where m is the message to be signed, w is the random integer with a range 1 to $p - 1$, and t is the reversible matrix, so that the great common divisor or GCD (t, n) =1. The signature {x, y} must be sent back to the interrogator, which must test whether

$$x^2 + ky^2 \equiv m \bmod n \tag{17}$$

A simulation of the proposed system with Lab-View is demonstrated in Figure 7. The processes can be summarized as follows:

1. Transponder and interrogator agree on parameters of the elliptic curve function;
2. The transponder sends a signal with digital signature to interrogator;
3. Interrogator verifies the signature.



Elliptic Curve Parameters
a 95
b 13
p 137
G.x 115
G.y 4
ECC Standard RND Parameter
n Bits (RND) 8
Verifier Private Key 91
Message 30

Original Message

30	0	0	0
0	30	0	0
0	0	30	0
0	0	0	30

$k = -u^2 \pmod n$
K -10000

Signature Verification

30	0	0	0
0	30	0	0
0	0	30	0
0	0	0	30

$x^2 + ky^2 \equiv m \mod n$

Elliptic Curve Parameters
Inverse S-Box Input 8
Inverse S-Box O/p 30
Transponder Private Key 5
Y1 83
X1 99
V21 45
V22 67
V11 51
V12 104

4x4 Reversible Key Matrix Generation

51	104	87	33
45	67	92	71
52	104	86	33
45	68	92	70

Random Number W 0 100 1

$x \equiv (t + mt^{-1}).2^{-1} \mod n$
$y \equiv (t - mt^{-1}).2^{-1}.w^{-1} \mod n$

$W^{-1} \pmod n$

X

37	105	47	32
81	11	56	73
121	105	100	32
81	95	56	126

Y

107	100	110	37
38	17	99	63
50	100	30	37
38	97	99	120

Figure 7. The proposed system layout implemented with Lab-View.

5. Experimental Results and Discussion

The quantitative/qualitative performance evaluation of both the traditional and proposed technique could be measured using various parameters, including (i) timing analysis, (ii) security analysis, and (iii) robustness to security attacks. In particular, timing analysis is among the critical points in any digital signature's schemes, namely, the encryption speed plays a vital role in real-time applications. The longer the encryption/decryption process is, the less suitable the method for some applications, such as video conferencing and live streaming. Thus, a comparison of the execution time of the proposed scheme and different digital signature schemes (signature generation) was conducted.

Figure 8 summarizes the comparison with the approach proposed by Al-Sewadi et al. [36], where their authentication algorithm based on NIST-DSA is performed. As readily seen in the figure, the resulting data highlight the high speed of applying the ECC with the OSS scheme with a key length of 1024. However, the proposed method is slightly faster than OSS–ECC as an additional level of S-Box is added to the total processing time. It is worth mentioning that for the RSA algorithm to achieve the same level of security as the ECC technique, it basically requires an increased key length. Although RSA introduces simple computations, the ECC depends on DLP with a lesser key length [37]. Table 2 summarizes the comparative results between RSA, OSS–ECC, and the modified OSS–ECC in signature computation time with respect to key length, which achieved the same security level for all compared schemes. Moreover, Table 2 shows the signature time between RSA, OSS–ECC, and modified OSS–ECC. It is clear that the proposed modification cost is slightly higher than OSS–ECC, as an additional step of S-box and reversible matrix is added to the traditional OSS–ECC scheme. Table 3 summarizes the performance comparison between RSA, EC–DSA, OSS–ECC, and the proposed digital signature. As can be seen, the OSS–ECC and the modified OSS–ECC have the best performance.

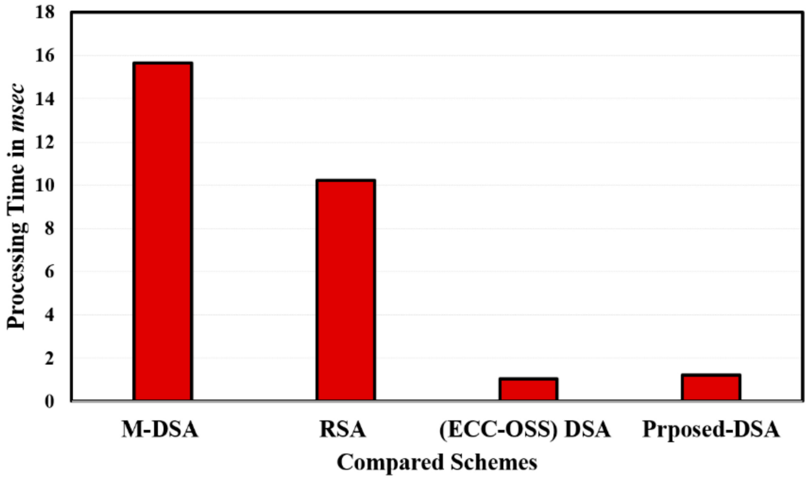


Figure 8. Comparison of total processing time of the proposed scheme and other state-of the-art schemes proposed in [32]. Note that "RSA", "DSA", "OSS", and ""ECC" stand for Rivest, Shamir and Adleman; digital signature algorithm, Ong, Schnorr, and Shamir; and elliptic curve cryptography, respectively.

Table 2. Signature generation computational cost (in milliseconds) of different signature schemes and the proposed scheme. Note that "RSA", "DSA", "OSS", and ""ECC" stand for Rivest, Shamir and Adleman; digital signature algorithm, Ong, Schnorr, and Shamir; and elliptic curve cryptography, respectively.

RSA		(OSS–ECC) DSA		Modified OSS–ECC	
KL	**Time**	**KL**	**Time**	**KL**	**Time**
1024	0.01	163	0.12452	163	0.125002
2240	0.15	233	0.13548	233	0.173998
7680	1.53	409	0.30213	409	0.326002
15,360	9.2	571	0.41568	571	0.483925

Table 3. Performance comparison between RSA, DSA, OSS–ECC, and proposed digital signature.

Scheme	Security	Complexity	Domain	Key Creator	Execution Time	Verify	Sign
RSA	High	Integer Factorization Problem (IFP)	PC, Laptops, and Super Computers	Medium	Slow	High	High
ECDSA	High	Discrete Logarithm Problem (DLP)	Lightweight Devices	High	High	Slow	High
OSS–ECC	High	(IFP–DLP)	Lightweight Devices	Higher	Highest	High	Higher
Modified OSS–ECC	High	(IFP–DLP)	Lightweight Devices	Higher	Highest	High	Higher

In addition to the timing analysis, the strength of the proposed S-Box was measured using two strong cryptanalytic attacks: differential and linear attacks. Typically, differential cryptanalysis aims to detect the "difference" between related encrypted plaintexts. The plaintexts may vary by a few bits. It attacks depending on a chosen plaintext: the attacker chooses the plaintext to be encrypted without the key, and then encrypts the related plaintexts [38]. The difference distribution tables of cyclic group sub-bytes were constructed, a worst case assumption was made in our consideration, which has a probability of 22/256 with input data difference $\Delta X = \{0, 1, 1, 1, 1, 0, 0, 0\}$, as illustrated in Table 4, except the cases of a one bit input/output difference, which are considered to be impossible (probability is zero). On the other hand, linear cryptanalysis exploits the high probability occurrences in bits of plaintext, ciphertext, and sub-key [39]. Such an expression takes the form:

$$x_1 \oplus x_2 \cdot x_u \oplus y_1 \oplus y_2 \cdot y_v = 0 \tag{18}$$

where x represents the input $x = [x_1, x_2 \ldots]$ and y represents corresponding output $\mathrm{y} = [\mathrm{y}_1, \mathrm{y}_2 \ldots]$. Equation (18) represents the exclusive-OR "sum" of u input bits and v output bits [40]. If the scheme shows a tendency to hold with high probability or not for Equation (18), this illustrates failure in randomization abilities [41,42]. The main factor that assesses the efficiency of the scheme is the linear probability bias, which is the amount of probability of a linear expression deviating from $\frac{1}{2}$. The higher the magnitude of the probability bias, $|\frac{1}{2} \pm \mathrm{P}_\mathrm{L}|$, the worse the security is [36]. In linear cryptanalysis, the relations between two bits of cyclic group sub-bytes can be found; the probability $(\frac{1}{2} \pm \mathrm{P})$ of these relations is restricted by $\frac{1}{2} \pm \frac{24}{256}$, as illustrated in Algorithm 1.

Table 4. Difference distribution table for input difference $\Delta X = \{0, 1, 1, 1, 1, 0, 0, 0\}$.

	Output Difference															
0 → 15	0	0	0	0	0	0	4	0	0	0	0	0	4	0	0	4
16 → 31	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	4
32 → 47	0	0	2	0	0	0	4	0	2	0	4	0	0	0	0	0
48 → 63	0	4	0	2	2	0	0	0	0	4	0	0	0	4	0	0
64 → 79	22	0	0	0	0	0	0	0	8	0	14	0	0	0	0	0
80 → 95	0	0	0	0	0	0	8	0	0	8	0	8	0	0	0	0
96 → 111	2	2	0	0	0	0	0	0	4	0	2	0	0	0	0	0
112 → 127	0	0	2	0	0	0	0	8	0	0	0	0	0	0	6	6
128 → 143	0	0	0	0	0	0	2	0	0	0	0	0	4	0	0	4
144 → 159	0	2	0	0	0	0	0	0	0	0	0	2	0	0	0	4
160 → 175	0	0	4	0	0	0	4	0	0	0	4	0	0	0	0	0
176 → 191	2	4	0	4	0	0	0	0	0	2	0	0	0	2	0	0
192 → 207	6	6	0	0	0	0	0	0	0	0	0	8	4	8	0	0
208 → 223	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0
224 → 239	0	0	0	0	0	0	0	0	2	0	6	0	8	0	0	0
240 → 255	2	2	0	0	0	0	0	2	0	8	0	0	0	0	0	0

Finally, the performance of the proposed technique can be evaluated by its robustness to security attacks, such as (i) brute-force, (ii) password sniffing, (iii) man-in-the-middle, and (iv) replay attacks. The former is the most popular public key attack, which tries to derive the private key from the know public key [43]. A given system is said to be secured against this type of attack if its key length is ≥70 bits with a probability of 2^{70} [44]. In the proposed scheme, the key length is considered to be the summation of the ECC key length with a probability of 2^{163} bits in addition to 2^7 generators of the proposed S-Box. Thus, the robustness of the proposed scheme implies that if a third party has the main parameters of EC function, $\{a, b, p, G\}$ and $\{P_A, k\}$, which are the public keys, it is not possible to estimate the signature {x, y} using trial and error with a probability of $2^{(163+7)}$ bits. Second, the password sniffing attack eavesdrops the network to intercept keys or passwords by capturing passing data. Attackers analyze data to predict keys. Encryption algorithms are the best way to be resilient against sniffing attack. The proposed scheme basically depends on the ECC, which works as a firewall against that types of attack.

Third, Pollard and Schnorr [18] succeeded in forging the signature without solving the quadratic equation. Their scheme approves its strength, as the signatures x and y are a 4×4 matrix with a large key length, which makes it hard to estimate. If a third party tried to estimate the second part of signature y where the attacker intercepts and/or modifies the data in transit, a constant value of x could be assumed. Here is a quadratic equation with a complex term. It is hard to calculate the square root to obtain y, while estimating

x and fixing the second part y equals factoring n. Such quadratic equation is difficult to solve, which can be explained in the following algorithm (Algorithm 1):

Algorithm 1 Steps for calculating quadratic equation roots

```
1. Given $n$ = P $\times$ Q, where {P, Q} are unknown prime numbers;
2. Choose w and Compute $\text{w}^{-1}$(mod $n$);
3. Scheme A: requires signatures of random messages (m) to run, and m must be signed using the private key $\text{w}^{-1}$;
4. Recall Scheme (A) using the signatures and the public keys {$k$, $n$};
5. $\text{w}^{'}$ is computed by scheme (A) as follows:
       $$-\,w'^{\,2} \equiv k \bmod \Phi(n); \qquad (19)$$
6. With a probability of $\frac{1}{2}w' = \pm w \bmod \Phi(n)$, the GCD$(\Phi(n),\ w' \pm w) > 1$ are the two prime numbers {P, Q};
7. According to the previous steps, if $w' \neq \pm\, w \bmod \Phi(n)$, then choose another ($w$) and reiterate all steps;
8. After ($n$) rounds, the possibility of computing the factorization is $1 - 2^n$.
```

Last, in replay attacks, the attackers try to intercept and record the plaintext. The captured data are used another time to try and recreate authentication. The hybrid ECC is used in the declared scheme, as the main parameters a, b, p, and G are generated randomly for each iteration, i.e., it has completely different signatures in each round. Therefore, the modified ECC–OSS approved its strength against this type of attack.

6. Conclusions

A hybrid scheme of an elliptic curve cryptosystem with a modified digital signature scheme was presented in this paper. A logistic map was used to produce the S-Box in addition to a reversible matrix as a portion of the OSS signature equation. The goal was to propose a robust scheme with minimal execution time. The illustrated results documented the robustness and efficiency of our technique against cryptanalysis in terms of implementation and security standardization. However, it requires a slightly longer processing time than DSA without S-Box due to the added complexity of combining the integer factorization problem and discrete logarithm problem. Moreover, the proposed scheme has a high immunity to resist the differential cryptanalysis. This scheme is comparable to existing, related schemes; it is also applicable to resource constrained devices, such as IoT network devices.

Author Contributions: A.T., M.A.M., A.S.S., and F.K.: conceptualization. S.H.A.E. and A.T.: methodology, formal analysis, and visualization. S.H.A.E., A.T., and F.K.: original draft preparation. S.H.A.E.: software and data curation. A.T., M.A.M., A.S.S., and F.K.: validation and supervision. A.T. and F.K.: investigation. A.T., S.H.A.E., M.A.M., A.S.S., and F.K.: review and editing final version. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available within the article.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DLP	Discrete Logarithm Problem
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
GCD	Great Common Divisor
IFP	Integer Factorization Problem
IOT	Internet of Things
IP	Internet Protocol
KP	Key Pair
MSP	Machine Service Provider
OSS	Ong, Schnorr, and Shamir
RNG	Random Generator
RSA	Rivest, Shamir, and Adleman
S-Box	Substitution Box
TTV	The Tree of Trust

References

1. El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) Authentication schemes. *Sensors* **2019**, *19*, 1141. [CrossRef] [PubMed]
2. Samaila, M.G.; Neto, M.; Fernandes, D.A.; Freire, M.M.; Inácio, P.R. Challenges of securing Internet of Things devices: A survey. *Secur. Priv.* **2018**, *1*, e20. [CrossRef]
3. Symanovich, S. The future of IoT: 10 predictions about the internet of things. *Cyber Secur. Blog Nort. Symantec Accessed* **2019**, 2–17. Available online: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html (accessed on 8 February 2021).
4. Naeem, M.; Chaudhry, S.A.; Mahmood, K.; Karuppiah, M.; Kumari, S. A scalable and secure RFID mutual authentication protocol using ECC for Internet of Things. *Int. J. Commun. Syst.* **2019**, *33*, e3906. [CrossRef]
5. Berndt, S.; Li'skiewicz, M. Algorithm Substitution Attacks from a Steganographic Perspective. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 1649–1660.
6. Raikwar, M.; Gligoroski, D.; Kralevska, K. SoK of Used Cryptography in Blockchain. *IEEE Access* **2019**, *7*, 148550–148575. [CrossRef]
7. Al-Mahmud, A.; Morogan, M. Identity-based Authentication and Access Control in Wireless Sensor Networks. *Int. J. Comput. Appl.* **2012**, *41*, 18–24. [CrossRef]
8. Malik, M.; Dutta, M.; Granjal, J. A survey of key bootstrapping protocols based on public key cryptography in the Internet of Things. *IEEE Access* **2019**, *7*, 27443–27464. [CrossRef]
9. Chen, L.Y.; Reiser, H.P. *Distributed Applications and Interoperable Systems*; Springer: Berlin/Heidelberg, Germany, 2017.
10. Ghofar, A.; Hardi, M.; Firdaus, M.N.; Shidik, G.F. Digital Signature Based on PlayGamal Algorithm. In Proceedings of the 2017 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, Indonesia, 7–8 October 2017; IEEE: New York, NY, USA, 2017; pp. 58–65.
11. Rabah, K. Security of the Cryptographic Protocols Based on Discrete Logarithm Problem. *J. Appl. Sci.* **2005**, *5*, 1692–1712. [CrossRef]
12. Farah, M.A.B.; Farah, A.; Farah, T. An Image Encryption Scheme Based on a New Hybrid Chaotic Map and Optimized Substitution Box. *Nonlinear. Dyn.* **2020**, *99*, 3041–3064. [CrossRef]
13. Guesmi, R.; Farah, M.; Kachouri, A.; Samet, M. Chaos-Based Designing of a Highly Nonlinear S-Box Using Boolean Functions. In Proceedings of the 2015 IEEE 12th International Multi-Conference on Systems, Signals & Devices (SSD15), Mahdia, Tunisia, 16–19 March 2015; pp. 1–5. [CrossRef]
14. Roy, S.; Khatwani, C. Cryptanalysis and improvement of ECC based authentication and key exchanging protocols. *Cryptography* **2017**, *1*, 9. [CrossRef]
15. Khatoon, S.; Rahman, S.M.M.; Alrubaian, M.; Alamri, A. Privacy-Preserved, Provable Secure, Mutually Authenticated Key Agreement Protocol for Healthcare in a Smart City Environment. *IEEE Access* **2019**, *7*, 47962–47971. [CrossRef]
16. Nikooghadam, M.; Amintoosi, H. Cryptanalysis of Khatoon et al.'s ECC-based Authentication Protocol for Healthcare Systems. *arXiv* **2019**, arXiv:1906.08424.
17. Rahim, R.; Pranolo, A.; Hadi, R.; Asyidah, R.R.; Nurdiyanto, H.; Napitupulu, D.; Ahmar, A.; Abdillah, L.; Abdullah, D. Digital Signature Security in Data Communication. *Adv. Intell. Syst. Res. (AISR)* **2017**, *144*, 172–177.
18. Pollard, J.; Schnorr, C. An efficient solution of the congruence $x^2 + ky^2 = m(\mathrm{mod}\ n)$. *IEEE Trans. Inf. Theory* **1987**, *33*, 702–709. [CrossRef]

19. Biswas, S. Enhancing the Privacy of Decentralized Identifiers with Ring Signatures. Master's Thesis, Aalto University, Espoo, Finland, 2020.
20. Shingala, K. An Alternative to the Public Key Infrastructure for the Internet of Things. Master's Thesis, Norges Teknisk-Naturvitenskaplige Universitet, Trondheim, Norway, 2019.
21. Shuo, C.; Ma, M.; Luo, Z. An authentication scheme with identity-based cryptography for M2M security in cyber-physical systems. *Secur. Commun. Netw.* **2016**, *9*, 1146–1157.
22. Singh, A.K.; Solanki, A.; Nayyar, A.; Qureshi, B. Elliptic Curve Signcryption-Based Mutual Authentication Protocol for Smart Cards. *Appl. Sci.* **2020**, *10*, 8291. [CrossRef]
23. Maletsky, K. RSA vs. ECC Comparison for Embedded Systems. 2015. Available online: http://ww1.microchip.com/ (accessed on 8 February 2021).
24. Seok, B.; Park, J.; Park, J. A Lightweight Hash-Based Blockchain Architecture for Industrial IoT. *Appl. Sci.* **2019**, *9*, 3740. [CrossRef]
25. Alzahrani, B.A.; Chaudhry, S.A.; Barnawi, A.; Al-Barakati, A.; Shon, T. An Anonymous Device to Device Authentication Protocol Using ECC and Self Certified Public Keys Usable in Internet of Things Based Autonomous Devices. *Electronics* **2020**, *9*, 520. [CrossRef]
26. Liu, Z.; Liu, D.; Zou, X.; Lin, H.; Cheng, J. Design of an elliptic curve cryptography processor for rfid tag chips. *Sensors* **2014**, *14*, 17883–17904. [CrossRef]
27. Satapathy, U.; Mohanta, B.K.; Jena, D.; Sobhanayak, S. An Ecc Based Lightweight Authentication Protocol for Mobile Phone in Smart Home. In Proceedings of the 2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS), Rupnagar, India, 1–2 December 2018; IEEE: New York, NY, USA, 2018; pp. 303–308.
28. Das, A. *Computational Number Theory*; CRC Press: Boca Raton, FL, USA, 2013.
29. Azarderakhsh, R.; Reyhani-Masoleh, A. Efficient FPGA implementations of point multiplication on binary Edwards and generalized Hessian curves using Gaussian normal basis. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2011**, *20*, 1453–1466. [CrossRef]
30. Wohlwend, J. *Elliptic Curve Cryptography: Pre and Post Quantum*; Technical Report; MIT, Tech. Rep: Atlanta, GA, USA, 2016.
31. Coppersmith, D.; Stern, J.; Vaudenay, S. Attacks on the Birational Permutation Signature Schemes. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 1993; pp. 435–443.
32. Ong, H.; Schnorr, C.P.; Shamir, A. An Efficient Signature Scheme Based on Quadratic Equations. In Proceedings of the Sixteenth Annual ACM Symposium on Theory of Computing, New York, NY, USA, 30 April–2 May 1984; pp. 208–216.
33. Wang, Y.; Liu, Z.; Ma, J.; He, H. A pseudorandom number generator based on piecewise logistic map. *Nonlinear Dyn.* **2016**, *83*, 2373–2391. [CrossRef]
34. Logachev, O.A.; Salnikov, A.A.; Yashchenko, V.V. *Boolean Functions in Coding Theory and Cryptography*; American Mathematical Soc.: North Providence, RI, USA, 2012; Volume 241.
35. Ruming, Y.; Jian, Y.; Jian, W.; Xiuming, S.; Xiqin, W. Designing key-dependent chaotic S-box with larger key space. *Chaos Solitons Fractals* **2009**, *42*, 2582–2589.
36. Guo, C.; Yong, C.; Xiaofeng, L. An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. *Chaos Solitons Fractals* **2007**, *31*, 571–579.
37. Ullah, I.; Hayat, U.; Bustamante, M.D. Image Encryption Using Elliptic Curves and Rossby/Drift Wave Triads. *Entropy* **2020**, *22*, 454. [CrossRef]
38. Al-sewadi, H.A.; Rifaat, M.M. Reduced time complexity variant of digital signature algorithm. *J. Theor. Appl. Inf. Technol.* **2018**, *96*, 1–94.
39. Bafandehkar, M.; Yasin, S.M.; Mahmod, R.; Hanapi, Z.M. Comparison of ECC and RSA Algorithm in Resource Constrained Devices. In Proceedings of the 2013 International Conference on IT Convergence and Security (ICITCS), Macao, China, 16–18 December 2013; IEEE: New York, NY, USA, 2013; pp. 1–3.
40. Conrad, E.; Misenar, S.; Feldman, J. *CISSP Study Guide*; Newnes: New South Wales, Australia, 2012.
41. Standaert, F.X.; Piret, G.; Quisquater, J.J. *Cryptanalysis of Block Ciphers: A Survey*; UCL Crypto Group: Louvain-la-Neuve, Belgium, 2003.
42. Ren, J.; Chen, S. Cryptanalysis of Reduced-Round SPECK. *IEEE Access* **2019**, *7*, 63045–63056. [CrossRef]
43. Heys, H.M. A tutorial on linear and differential cryptanalysis. *Cryptologia* **2002**, *26*, 189–221. [CrossRef]
44. Van Tilborg, H.C.; Jajodia, S. *Encyclopedia of Cryptography and Security*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2014.