Robustness Analysis of Zero-Knowledge Proofs using QRP for IoT Devices

Chitranjan Prasad Sah
CSE-APEX, Chandigarh University
Gharuan, Mohali, Panjab, India
chitranjan.e12706@cumail.in

***Abstract*— We attempt to study the time complexity and asymptotic security of the method in order to robustly analyze the security mechanism. Security analysis studies allow us to determine whether an algorithm is efficient or not. Security analysis studies also help us check whether algorithms tolerate different attacks on them or not. This research paper presents the robustness analysis of the zero knowledge proofs (ZKP) technique using the quadratic residuosity problem (QRP) as a superior alternative for Internet of Things (IoT) devices. If we want to achieve the main security issues (attacks on confidentiality, authentication, integrity, and availability) for IoT devices, then we need to know the security strength of the security mechanism we implement for it. The zero-knowledge proofs technique has been used with the QRP problem, and it is analyzed and compared with Elliptic Curve Cryptography (ECC) in order to see how they are correlated with each other. This study helps us know whether ZKP using QRP can address the security issues of IoT devices in a better way or not. The final covariance and correlation results show that both ZKP using QRP for the square root modulo n problem (SQROOT) and ECC are highly correlated with one another. Asymptotic time complexity and the graph of ZKP using QRP for the SQROOT algorithm compared to ECC clearly show that QRP for the SQROOT algorithm has not as good a time complexity as ECC but can address the security issues required by IoT devices.**

Keywords— Elliptic curve cryptography, IoT, oblivious transfer, Pollard's rho algorithm, QRP, security, zero-knowledge proofs.

I. Introduction

Most businesses and organisations use sensor-enabled Internet of Things (IoT) devices for instant messaging and communication in the age of wireless sensor networks and IoT devices to integrate messaging and IoT services. The IoT devices for instant messaging and communication help us to enhance better user experience and friendliness. The IoT devices connected to the internet are vulnerable to different types of security attacks and privacy violations [15]. This happens when messages are exchanged through base stations that are connected to public networks, short message services, and mobile switching centres. The technologies and gadgets utilised in IoT environments are the main causes of security problems in IoT devices. The primary security vulnerabilities that can be seen in an IoT environment are attacks on confidentiality, authenticity, integrity, and availability. Messaging also opens the door for replay attacks, message interception, sniffing, and data origin impersonation. Secure access control for the restricted resources was designed and implemented using the authentication by zero knowledge proofs method [16, 23, 25, 26].

So, using the quadratic residuosity problem, I have examined the robustness of the zero knowledge proofs technique in this research. QRP will be a better choice for IoT devices to address the primary security challenges, as indicated before. A non-black box cryptographic technique known as "zero-knowledge proof" allows two parties to communicate with one another in order to establish a claim without disclosing their own secrets [4, 10, 12]. The zero-knowledge proofs by means of QRP have been analyzed and compared with elliptic curve cryptography in order to see how they are correlated with each other. This enables us to determine whether or not zero-knowledge proofs using the QRP problem can effectively address the security concerns of IoT devices. For random input size values, the time complexities of ECC and zero knowledge proofs using the SQROOT algorithm are compared, and a graph between them is produced to show the relationship between them. Finally, we can conclude that zero-knowledge proofs using the SQROOT algorithm's QRP can be used as an ECC substitute and can better handle the security needs of IoT devices than ECC.

II. Background

In the first place, we need to take care of server authentication as well as user authentication if we want to adopt trustworthiness in IoT communication systems to ensure the vital goals that are required for information security.

As we all know, authentication is a system through which a person can independently verify his or her identity during a conversation and assure the validity of the communication's starting point. The basic objective of a security system is to operate as a security guard before any other security device in order to stop various hacker assaults and malfunctions. Therefore, a new form of authentication method must be created and used in order to authenticate both people and devices during the connection of various types of devices.

Commercial applications often use one of four sorts of authentication mechanisms: something you know, something you have, something you are, and someplace where you are. Therefore, the most popular method of user identification is to enter their user ID and passcode and submit them through a Secure Socket Layer connection. Computing systems generate cryptographic hashes to send passwords over public networks rather than plain text. As a result of the availability of wired and wireless internet, however, the hashed credentials sent across public networks are not safe and can be accessed by hackers and invaders. Additionally, a 3G GSM connection is not secure and can be broken in just two hours. Therefore, we require a certain

978-93-80544-47-2/23/©BVICAM, New Delhi, India

kind of security system that can demonstrate security without revealing our secret authentication code.

As is generally known, the traditional authentication process takes time, resulting in some overhead on both the server and the end user's computer. Research is currently being done to discover a solution for smart devices with low memory and battery capacity in an effort to lessen this problem. This study demonstrates the robustness of the zero-knowledge proofs technique using the QRP algorithm and how it is appropriate for the security and performance requirements of the Internet of Things [17, 18].

Furthermore, research on IoT devices reveals that the majority of them are used without any kind of password or authentication system. Weak password usage and traffic encryption are the main problems with IoT devices [19]. Most consumers in this digital age use their mobile devices to do banking business, make payments, and shop. Protecting their identification is essential in order to assure authentication [20].

The IoT enables a variety of network types as well as different types of entities because devices can communicate with each other, with humans, and with other humans. Because SSL communication is not enabled in this domain and IoT devices have no prior knowledge of other entities, it is feasible to eavesdrop on conversations. Additionally, IoT smart devices are linked to many kinds of sensors and actuators in order to exchange and gather the necessary information for authentication, increasing the risk of identity disclosure or access by unauthorised parties. We thus require a special kind of authorisation and access control systems in order to secure personal data as well as anonymity support. As is well known, there is a serious issue with discrimination in sensor output, and there is no IoT privacy rule in place.

As is well known, under prior authentication schemes, clients had to provide their user names and passwords to the server by hashing their credentials over a public network. The server sends acknowledgement packets to the client across a public network as well. Furthermore, the public networks used for the transfer of these credentials, including 4G mobile broadband, Wi-Fi, and ZigBee, are open to hacker attacks. Therefore, a hacker can intercept the credentials that we send over a public network, and the compromised credentials may be used to steal important data from servers, launch security attacks against the server to halt its services, or use password recovery software to recover the password by reversing hashes.

The various kinds of authentication systems can be roughly divided into three groups. They rely on one-time signatures, public keys, and either private keys or public keys with one-time signatures. Public key-based authentication is therefore more secure than one time signature and private key techniques, and it can be employed with zero-knowledge proofs to reduce the need for significant compute, communication, and storage overhead [21, 24].

IoT devices need a special security method because of their portability, wireless connections, and network access layer links between their components. As a result, zero-knowledge knowledge proof using QRP is preferable for this kind of gadget.

Full-sized security secret statements (codes) are divided into two parts for this kind of security authentication system, and proofs can be made between the user and system through a non-interactive communication process. This is a better idea for higher security because some information will be with smart users and the rest will be inside the smart IoT devices. The following is the key concept underlying this security method utilizing the QRP problem:

(1) The smart devices will only have one instance of a QRP challenging difficulty, *i.e.,* a set J_n, which is the set of all $a \in \mathbb{Z}_n^*$ having the Jacobi symbol 1 and an odd composite integer *n*.

Users of smart IoT devices need to know the answer to a QRP hard problem, which is a number that is a quadratic residue modulo *n* and is represented by the variable *a*.

(2) Authenticated users must complete the security proofs and difficulties provided by the QRP mathematical problem utilizing secret codes and zero-knowledge proofs in order to gain access to smart devices. [3, 2, 10].

III. Mathematical Notations

Set: Sets are collections of clearly specified elements. Members or elements of a set are items that are a part of it. English capital letters like A, B, Y, and Z, among others, are used to symbolize it. We primarily use two sets in cryptography: $\mathbb{Z}_p$and $\mathbb{Z}_p^*$ for some integer *p*. Both of these sets utilize a prime number as the modulus. $\mathbb{Z}_p$ contains all integers from 0 to $p - 1$ whereas $\mathbb{Z}_p^*$ contains all integers from 1 to $p - 1$. Except that *n* is a prime, the set $\mathbb{Z}_p^*$ is the same as $\mathbb{Z}_n^*$. Each member in $\mathbb{Z}_p^*$ has an additive and multiplicative inverse. For example, when *p* = 7, we have $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, and $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ [1, 6, 11].

Quadratic residue: If this congruence has a solution for an integer $0 < x < p$, such that $x^2 \equiv q \pmod{p}$, then *q* is called a quadratic residue (mod *p*) otherwise *q* is called quadratic nonresidue (mod *p*). For example, $10^2 \equiv 1 \pmod{11}$ means that 1 is a quadratic residue (mod 11). Therefore, all possible quadratic residues are: 1, 3, 4, 5, and 9, since $10^2 \equiv 1 \pmod{11}$, $6^2 \equiv 3 \pmod{11}$, $9^2 \equiv 4 \pmod{11}$, $4^2 \equiv 5 \pmod{11}$, and $8^2 \equiv 9 \pmod{11}$. 2, 6, 7, 8, and 10 are quadratic nonresidues (mod 7) [11, 9].

Big–O notation: Assume that $g(n) \in O(h(n))$, $c \in R^+$, and also $x_0 \in N$ such that $0 \leq g(n) \leq ch(n)$ relationship valid for $n > x_0$. $g(n) \in O(h(n))$ expression reads as "*g* (*n*) is big–*O* of (*n*)". The upper bound on the time complexity of algorithms is analyzed using this asymptotic notation to determine how long an algorithm will take the CPU to run.

Covariance: Covariance is frequently used in the statistical and probability mathematical domains to measure the link between two random variables and the degree to which they change together in order to determine how two separate sets of random variables are related to one another. Covariance tells us whether one set of random variables reflects favourable behaviour with another set of random variables. If the first group of random numbers has smaller values that match the second group's smaller values, and vice versa, if the first group's larger exhibiting similar behaviour to one another, and we will receive a positive covariance result in this case. And if smaller values of the first group of random numbers correspond with larger values of the second group of random numbers, and vice versa, we will obtain a result of covariance as a negative number, which indicates that both sets of variables are showing conflicting behaviour with one another.

IV. Zero Knowledge Proofs

'Zero-knowledge Proofs are both convincing and yet yield nothing beyond the validity of the assertion being proven, which is the idea on which the zero-knowledge proofs technique is based, and it was first presented in 1982 by Goldwasser, Micali, and Rackoff [2]. So, in other words, we can say that zero knowledge proof is a type of security proof technique in which two different communicating parties communicate with each other in such a way that one party can prove to the other party that he or she knows a secret without revealing the secret to the other party. The non-interactive communication with the prover (P) has completely convinced the verifier (V) that the claim is true [8]. Completeness, soundness, and zero knowledge are the three key characteristics of ZKP.

The safe indirect route of communication between V and P is a form of non-interactive communication, which is the process of exchanging messages [7]. As a result, we may utilize the oblivious transfer technique to make entity p and entity V's communication non-interactive, which is the most crucial criterion for the ZKP technique. This idea was put forward by Rabin et al., who claimed that we could easily make the ZKP approach non-interactive with the aid of oblivious transfer. Details on how we can use oblivious transfer to make ZKP non-interactive are provided in [5, 7, 13].

V. Quadratic Residuosity Problem

A quadratic residuosity problem is defined as: if someone wants to know whether a is a quadratic residue or not for a given n, which is an odd composite integer number, and $a \in J_n$, where if $n \geq 3$, then J_n is the set of all $a \in \mathbb{Z}_n^*$ with Jacobi symbol 1[3]. QRP with a prime modulus is defined as: if n is a prime, then it is easy to decide whether $a \in \mathbb{Z}_n^*$is a quadratic residue modulo n since, by definition, $a \in Q_n$if and only if $\left(\frac{a}{n}\right) = 1$ and the Legendre symbol $\left(\frac{a}{n}\right)$ can be can be efficiently calculated by Algorithm 2.149. where Q_n is the set of quadratic residues modulo n. Assume now that n is a product of two distinct odd primes, p and q. It follows from fact 2.137 that if $a \in J_n$ then $a \in Q_n$ if and only if $\left(\frac{a}{n}\right) = 1$. Thus, if the factorization of n is known, then QRP can be solved simply by computing the Legendre symbol $\left(\frac{a}{n}\right)$. This observation can be generalized to all integers and leads to the fact that QRP $\leq_p$ FACTORING that is the QRP polytime reduces to the factoring problem [3].

VI. Robustness of Zero Knowledge Proofs using QRP Problem

When analysing the resilience of a cryptographic security mechanism, we always try to determine the time and space complexity of the mathematical operations performed inside the security algorithm is stronger than the other and whether it can tolerate various types of adversarial attacks or not, time complexity is more crucial than space complexity. To meet this need, we can utilize asymptotic notation (big-O) to determine the time complexity of the mathematical operations employed to solve the integer factoring issue. From this information, we can learn about the speed and efficiency of the CPU.

Due to the employment of zero-knowledge proofs as a security measure in the QRP problem, the running time required to compute the product of two separate odd primes, a and b, dominates the execution time. The *square root modulo n problem* is a special kind of mathematical problem where we find the square root of a modulo n.

Given a composite integer n and a quadratic residue a modulo n (i.e., $a \in Q_n$), we can calculate the square root of a modulo n. The SQROOT problem can be effectively solved if the factors p and q of n are known by first determining the square roots of a modulo p and modulo q. To find the square roots of a modulo n, combine them using the Chinese remainder theorem (Fact 2.120).

If we use "Finding square roots modulo n given its prime factors p and q" [3, algorithm 3.44] then the expected running time of this algorithm will be in bit operations as in the following equation (1).

$$ExpCost_{\mathbb{G}}(p) = (\lg p)^3 \qquad (1)$$

Elliptic Curve Cryptography (ECC), which is one of the best alternatives for data security in an IoT environment due to quick calculation and small key size, was employed for the comparative analysis of the SQROOT problem-related technique as indicated above. As a result, the time complexity of ECC is $O\sqrt{q}$ given in [14, 22].

A. Asymptotic Cost Comparison

TABLE I. Cost Compaision Table

Operation	SQROOT algorithm
	Asymptotic Cost
$\mathrm{ExpCost}_{\mathbb{G}}(\mathrm{p})$	$(\lg \mathrm{p})^3$
	Elliptic Curve Cryptography algorithm
	Asymptotic Cost
$\mathrm{ExpCost}_{\mathbb{G}}(\mathrm{p})$	$\mathrm{p}^{1/2}$

For the same reason, Table I presents the CPU cost of the SQROOT algorithm used in this paper and other algorithms used in elliptic curves so that we can compare them. The SQROOT algorithm is not more efficient than the elliptic curve cryptography technique, but it can be used as a better alternative for the increased security required in IoT devices [3, 14].

B. Comparison Graph

Table II calculates asymptotic functional values for the SQROOT algorithm and the Elliptic Curve Cryptography techniques to show the relationship between the functional values and the comparison graph.

TABLE II. FUNCTINAL VALUES CALCULATION

Input Size **(p)**	**SQROOT** **$(\lg p)^3$**	**ECC** **$p^{1/2}$**
109	310.29	10.44
211	460.28	14.53
366	617.60	19.13
474	702.36	21.77
693	840.43	26.32
962	973.24	31.02

This section compares the time complexity of the elliptic curve cryptography algorithm with the SQROOT algorithm for quadratic residuosity problems in order to understand how the graphs behave relative to one another when the same numerical inputs are applied to each technique. Fig. 1 shows the relationship graph between them.

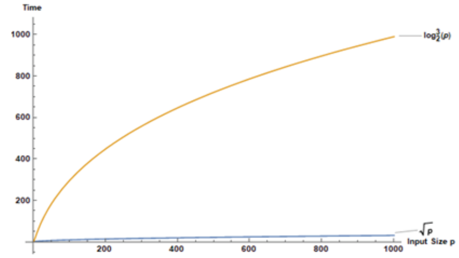

Fig. 1. The Time Complexity of Pollard's rho and ECC

C. Covariance between Asymptotic Costs

We must utilize a statistical tool called covariance, which allows us to understand the relationship between two sets of variables, in order to examine how two sets of random variables are expressing their nature with respect to one another. Therefore, covariance has been used to determine the relationship (correlation) between two sets of variables of asymptotic functions of the SQROOT method for QRP and elliptic curve cryptography techniques with the same input size. This relationship helps us to analyze how both asymptotic functions are showing their nature with respect to one another. The average cross product of one group of random variables with a second group of random variables, which has been derived for the aforementioned asymptotic functions as follows, is known as covariance.

TABLE III. FUNCTINAL VALUES CALCULATION

Input Size **(p)**	**$(\lg p)^3$** **(P)**	**$p^{1/2}$** **(S)**
109	310.29	10.44
211	460.28	14.53
366	617.60	19.13
474	702.36	21.77
693	840.43	26.32
962	973.24	31.02

The average values of P and S from table III are now calculated; P and S are denoted by the letters E[P] and E[S], respectively. So, the calculated mean value of P is E[P] = 650.7 and the calculated mean value of S is E[S] = 20.54, and the values of E[P] and E[S] have been used in the following Table IV in order to compute the deviated value from their average value, which can be represented by Q and R.

TABLE IV. DEVIATION FROM MEAN

$(\lg p)^3$ **(P)**	**A − E[A]** **(Q)**	**$p^{1/2}$** **(S)**	**B − E[B]** **(R)**
310.29	-340.41	10.44	-10.1
460.28	-190.42	14.53	-6.01
617.60	-33.1	19.13	-1.41
702.36	51.66	21.77	1.23
840.43	189.73	26.32	5.78
973.24	322.54	31.02	10.48

Here, we determine the cross multiplication of Q and R in Table V, which is determined by multiplying the numeric value of Q with the corresponding numeric value of R from Table IV.

TABLE V. CROSS PRODUCT Q AND R

$Q * R$	**Cross − Product**
(-340.41) * (-10.10)	3438.14
(-190.42) * (-6.01)	1144.42
(-33.1) * (-1.41)	46.67
(51.66) * (1.23)	63.54
(189.73) * (5.78)	1096.64
(322.54) * (10.48)	3380.22
Total Sum	9169.63

The results of the cross-product of Q and R as well as the total cross product are shown in Table V. In order to determine the covariance between P and S, the total sum of the cross product must be divided by $df(n-1)$. The calculated covariance result is 1833.93 as a consequence. Positive covariance between P and S is the end result. Additionally, the correlation between P and S is calculated, and the outcome is 0.9987. The results of covariance and correlation indicate that the nature and rate of growth of both problems are comparable.

VII. Conclusion

The zero-knowledge proofs using QRP and ECC are examined in this study paper to understand how they relate to one another. And the covariance and correlation between QRP for the SQROOT algorithm and ECC are 1833.93 and 0.9987, respectively, which clearly show that both problems are highly correlated with one another and have a similar nature. But, the time complexity of QRP for the SQROOT algorithm is higher than ECC, which is a negative part of this algorithm. The QRP problem has been used with the zero knowledge proofs technique, so we can select a medium-sized composite number n for the QRP problem in order to enhance the time complexity for IoT devices. Therefore, it is important to consider the bit size of composite numbers when choosing them in order to provide stronger security for IoT device authentication and alleviate the bottleneck issue. For values of the random input size, a graph between them is created to help us understand the clear relationship between them. Finally, we can say that zero-knowledge proofs using QRP for the SQROOT algorithm are a better alternative to ECC and can address the security issues required by IoT devices in a better way. This research study will benefit academics and research personnel working in the non-interactive security sector by providing a fresh approach to advance the field of cryptography and advance resettable cryptography.

Acknowledgment

I want to thank my mother Paspati Devi Kalwarin and father Shambhu Sah Kalwar for her/his prestigious cooperation and love.

References

[1] O. Goldreich and Y. Oren, "Definitions and properties of zero-knowledge proof systems," Tech. Rep. TR-610, Haifa, Israel, 1990.

[2] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," SIAM J. Comput., vol. 18, No. 1,

[3] A.J. Menezes, S.A. Vanstone, and P.C. Van Oorschot, Handbook of Applied Cryptography. Boca Raton, CRC Press, Inc., FL, USA, 1996.

[4] R. Henry, "Efficient zero-knowledge proofs and applications," Ph. D. thesis, University of Waterloo, Ontario, Canada, 2014.

[5] N. Koblitz, A course in Number Theory and Cryptography, 2nd ed., Springer-Verlag, New York, Inc., 1994.

[6] B. Kolman, R.C. Busby, and S.C. Ross, Discrete Mathematical Structures, 5th ed., Prentice Hall, India, 2003.

[7] M. Blum, A.D. Santis, S. Micali, and G. Persiano, "Noninteractive zero-knowledge," vol. 20, No. 6, pp. 1084-1118, December 1991.

[8] B. Barak, "Non-black-box techniques in cryptography," Ph. D. thesis, Weizmann Institute of Science, Rehovot 76100, Israel, 2004.

[9] J. Katz, V. Koilesnikov and X. Wang, "Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures," University of Maryland and Georgia Tech, March 2019.

[10] C. P. Sah, P. R. Gupta, "Robust comparative analysis of zero-knowledge proofs using discrete logarithm problem," Proceedings of the 14th INDIACom, INDIACom-2020, 7th International Conference on Computing for Sustainable Global Development, March 2020.

[11] C. Peter Schnorr, "Efficient identification and signatures for smart cards," In Proceedings of CRYPTO 1989, vol. 435 of LNCS, pp. 239–252, Santa Barbara, CA, USA, August 1989.

[12] O. Goldreich," Zero-knowledge twenty years after its invention," Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rohovot, Israel, December 2002.

[13] M. Bellare and S. Micali, "Non-Interactive Oblivious Transfer and Applications," Advances in Cryptology - CRYPT0 '89, LNCS 435, pp. 547-557, 1990.

[14] S. Chandel, W. Cao, Z. Sun, J. Yang, B. Zhang, and T. Yi Ni, "A multi-dimensional adversary analysis of RSA and ECC in blockchain encryption," Springer Nature Switzerland AG 2020, pp. 988–1003, 2020.

[15] T. Borgohain, U. Kumar, S. Sanyal, "Survey of security and privacy issues of Internet of Things," Int. J. Advanced Networking and Applications Volume: 6 Issue: 4, pp. 2372-2378, 2015.

[16] R. Rehiman, S. Veni, "A secure authentication infrastructure for IoT enabled smart mobile devices – An initial prototype," Indian Journal of Science and Technology, Vol9(9), DOI: 10.17485/ijst/2016/(9)/86791, ISSN (Print) : 0974-6846ISSN (Online) : 0974-5645, March 2016.

[17] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "DTLS based security and two-way authentication for the internet of things," Elsevier Journal of AdHoc Networks, 11(8):2710-23, Nov 2013.

[18] R. Gogha, S. Prateek, N. Kataria, "Home automation: Access control for IoT devices," International Journal of Scientific and Research, 4(10), Oct 2014.

[19] J. -Y. Lee, W. -C. Lin and Y. -H. Huang, "A lightweight authentication protocol for Internet of Things," *2014 International Symposium on Next-Generation Electronics (ISNE)*, 2014.

[20] R. Hummen, H. Shafagh, S. Raza, T. Voigt, K. Wehrle, "Delegation based authentication and authorization for the IP based Internet of Things," IEEE 2014.

[21] K. A. Rafidha Rehiman and S. Veni, "A secure authentication infrastructure for IoT enabled smart mobile devices – An initial prototype," Indian Journal of Science and Technology, vol. 9, March 2016.

[22] P. C. Sethi, and N. Sahu, P. K. Behera, "Group security using ECC," International Journal of Information Technology (BJIT), vol. 14(2), pp. 955–963, March 2022.

[23] Z. Baloch, F. K. Shaikh, and M. A. Unar, "A context-aware data fusion approach for health-IoT," International Journal of Information Technology (BJIT), vol. 10, pp. 241–245, 2018.

[24] A. Khiat, A. Bahnasse, J. Bakkoury, M. El Khaili, F. E. Louhab, "New approach based internet of things for a clean atmosphere," International Journal of Information Technology (BJIT), vol. 11, pp. 89–95, 2019.

[25] V. Bhasin, S. Kumar, P. C. Saxena, and C. P. Katti, "Security architectures in wireless sensor network," International Journal of Information Technology (BJIT), vol. 12, pp. 261–272, 2020.

[26] P. Matta, and B. Pant, "TCpC: a graphical password scheme ensuring authentication for IoT resources," International Journal of Information Technology (BJIT), vol. 12, pp. 699–709, 2020.