E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 01-06-2023
Accepted: 06-07-2023

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 1; Issue 1; 2023; Page No. 650-654

Cryptanalysis of pre-quantum and post-quantum cryptography

[1]Ranjita and [2]Dr. Gautam Kumar Rajput

[1]Research Scholar, Sunrise University Alwar Rajasthan, Rajasthan, India
[2]Associate Professor, Sunrise University Alwar Rajasthan, Rajasthan, India

DOI: https://doi.org/10.5281/zenodo.13643131

Corresponding Author: Ranjita

Abstract

Cryptanalysis, the study of analyzing and breaking cryptographic algorithms, has long been a crucial aspect of securing digital communications. As quantum computing approaches practical implementation, the cryptographic landscape is poised for significant transformation. This paper delves into the cryptanalysis of both pre-quantum and post-quantum cryptographic systems, highlighting the vulnerabilities and strengths of various algorithms in the face of evolving threats. Pre-quantum cryptography, which includes widely used systems like RSA and Elliptic Curve Cryptography (ECC), is based on mathematical problems that are hard to solve using classical computers. However, quantum algorithms, such as Shor's algorithm, pose a direct threat to these systems by potentially breaking their security within a feasible timeframe. In response, post-quantum cryptography is being developed to offer resistance against quantum attacks. This paper examines the cryptanalysis techniques applicable to these new algorithms, including lattice-based, hash-based, code-based, and multivariate polynomial cryptosystems.

Keywords: Cryptanalysis, cryptographic, quantum, elliptic curve cryptography, pre-quantum and post-quantum

Introduction

Cryptography is become an essential part of our daily lives. Cryptography is an essential part of our digital infrastructure that helps to protect our bank information, e-mail, and phone calls. There are often two components to modern cryptography. During the key exchange phase, a shared secret key is generated using a technique like RSA or Elliptic Curve Diffie-Hellman key exchange (ECDH). This key may then be used in the second phase of the encryption process, which is symmetrical. When instantiated with appropriate parameters and executed safely, these algorithms have been and will be extensively examined for their safety.

There are essentially two types of cryptographic assaults. One of them is to mathematically examine the implementation's cryptography algorithms. Section of this thesis will address a few of these assaults. Attacks that use side channels make up the second category. These attacks target the cryptographic operation's actual execution as opposed to its mathematical structure or protocol functionality, in an effort to uncover vulnerabilities. Device power throughput, electromagnetic radiation, audio recording, and the time of these measures are all examples of physical channels. Consider a method that uses a personal key k, a random number generator g, and a prime figure p to calculate the public key, as shown as gk mod p. We may then deduce that the key k = 1 makes this process much simpler than the key k = 011001000110100101100011011010101. However, Both implementation steps must take the same length of time for the security measure to be effective in preventing an adversary from getting critical information. Enhancing the attack strength by incorporating mathematical understanding of cryptography key, primitive, or protocol into side channel physical information is possible.

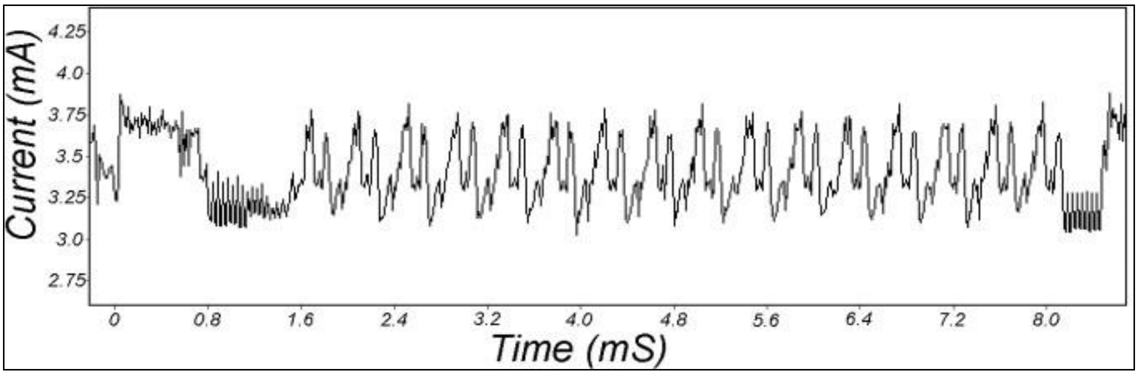

Fig 1: A DES operation's SPA trace as reported in [KJJ99].

Literature review

Dorostkar, Zahra. (2023) [1]. Mathematics for Cryptography: A Guide to Mathematical Principles of Various Cryptography Algorithm Classes. Even so, the piece does not go into great into on particular algorithms, its goal is to get readers acquainted with the basic ideas and principles that are necessary for comprehending each of these algorithms. This article presents a general outline of the mathematical backgrounds required by different cryptography algorithms. Its goal is to give readers a head starts so they can delve deeper into these algorithms and take part in the continuous investigation and advancement inside this ever-evolving sector.

Wu, Huangwei. (2023) [2]. A summary of elliptic curve encryption's basic mathematical ideas. Elliptic Curve Cryptography (ECC), primarily the ECC algorithm included in the source code of Bitcoin, is crucial to the current public-key cryptosystem. Due to the use of Diffie-Hellman key exchange and discrete logarithm, ECC has gradually advance to a state where it is both smart and efficient. Consequently, it is now generally considered the inherited successor of the RSA algorithm because to its lower key lengths, quicker speed, and greater safety at the same SSL level. There seems to be a great amount of mathematics concepts associated with the development of the ECC algorithm, which is understandable given the complexity and possible security of the Elliptic Curve Cryptosystem. Consequently, this paper will primarily make use of empirical study and case studies to clarify the fundamental principles of ECC, including the Law of Addition, ECDLP, and EC ElGamal, as well as their respective applications and deprivation procedures.

A, Anjali & L C, Manikandan. (2020) [7]. Exploring Cryptographic Methods Currently, it is a strain to provide proper network security situation, making it difficult to keep data safely online. Maintaining data secrecy is a complex art. Data security via communication channels is becoming more important as technology advances at a rapid pace. To ensure the safety of data transmission, many cryptographic methods are used. To guarantee the app has the required security, the cryptographic method and a number of algorithms are used. The field that studies how to encrypt and decode data is known as cryptography. Every single cryptographic method is laid forth in great depth in this work.

Mohammed, Abdalbasit & Varol, Nurhayat. (2019) [11]. As the internet has grown exponentially over the last several decades and has grown in importance to the point that data security is now a as a major issue for everyone with an online connection. Our data is protected against unauthorized access and modification by using robust data security measures. We have created a number of techniques and approaches to reach this degree of security. Cryptography is the practice of encrypting data using well-established techniques in a way that cannot be understood by humans unless more encryption is applied.

Hamlin, Nathan. (2017) [4]. An examination of representation and numbers sufficient for the job is required considering the imminent threat posed by quantum computing. This is applicable to the foundations of digital integer representations and here we clarify the combinatorial component of representation., by extension, to the question of what numbers are and their applications in both mathematical theory and practice. Mathematicians and computer scientists, according to the author, may have a better grasp of number theory and its applications by reading this book. The author is especially hopeful that it will shed light on the Characteristics of the Generalized Knapsack Code, a code based on lattice structure.

Selvam, Anitha & Padmalatha, Ms. (2022) [5]. An Investigation into Cryptography and Network Security. A key component of network security is ensuring the confidentiality of a message's contents via the use of cryptography during wireless transmission. Secure data transmission across an unstable network is primarily concerned with data security. The administrator of a network is responsible for ensuring the network safety via managing data access privileges. Many different types of computer networks, both public and private, make use of network security measures. When data arrives at its destination, it uses a mathematical representation called a hash function to determine the value of the data. Cryptography is the method used to secure data. Cryptography, therefore, is a new technology that is crucial to the safety of any network. The limited use of encryption in the past was to safeguard sensitive military data, diplomatic communications, and national security. The evolution of communication has greatly broadened the scope of cryptography's current uses in this contemporary field. When it comes to protecting sensitive information and doing business online, cryptography is an absolute must.

Manipulating bada55 curves

Internet traffic is becoming encrypted. Because of this, government authorities will be unable to effectively monitor Internet traffic in order to combat terrorism and transnational crime, which is a major concern for our society. For instance, most contemporary chat apps encrypt all communication, and more and more servers employ Standard Transport Layer Security (TLS) (not limited to data transfers including sensitive credentials or financial details). As a result, gathering the essential data at the endpoints-the servers or the clients-increases the cost of defending society. Because of this, agencies must either find a way to get the service providers to provide the requested data or install a backdoor on the client's machine. Agencies would save a lot of money if they just collected unprotected data from the transmission line instead of doing any of those things.

The good news is that, if agencies operate under acceptable assumptions, they can trick individuals into using cryptographic systems that they think are safe, but which the agencies can easily crack.

This chapter takes a dark approach by exploring potential social side channels for attacking cryptosystems that rely on elliptic curves. An evil actor may influence the decision-makers in charge of selecting elliptic curves for these systems, increasing the likelihood that a curve with a hidden vulnerability would be promoted. The number of possible curves is limitless. This chapter explores the extent to which this is feasible by looking at standardization methods and algorithms for curve creation.

Outside of this part, we consistently put ourselves in the shoes of the attacker. Before anything else, we want to make it clear that we do not support from the perspective of the assailant. We aim to evaluate system safety in order to forestall attacks. Secondly, under different circumstances, this chapter examines the potential for backdooring curves. Regarding the veracity of such an assault, we are remaining silent.

Alphabetic-curve Encryption

The reputation of elliptic-curve cryptography (ECC) as a highly secure method is contributing to its rising popularity. We use the elliptic-curve Diffie-Hellman (ECDH) key-exchange protocol, and in particular "ephemeral ECDH" for certainty, since it is generally thought to be the best way to achieve forward secrecy. Key exchange protocol ECDHE, P, using an elliptic curve E and a point P is the one most often used to simulate ephemeral ECDH in the literature.

1. Alice assigns the atomic multiple of P to E and creates a private integer a.
2. Bob generates a one-of-a-kind integer b and sends it as bP..
3. The ath multiple of bP is used by Alice to calculate abP.
4. The bth multiple of aP is what Bob uses to calculate abP.
5. Alice and Bob use abP to generate an encryption key.

No matter how robust the encryption, this protocol has been shown in several published attacks to be breakable for a wide variety of elliptic curves E. For information. Having said that, there are a plethora of (E, P) that have no security issues reported in the public domain. The same is true for elliptic-curve signatures and similar examples.

The origin of the curve (E, P) is an open issue in this concept. As far as most people are concerned, the solution is that one entity creates a curve and then touts the public's improved performance and security. 1 Our The fundamental objective of this research is to analyze potential public acceptance scenarios and their effects on security; nevertheless, this in no way suggests that people would blindly adopt curves. In the grand scheme of things, ECDHA is a three-party protocol in which A is a function, and Alice, Bob, and Jerry—the central authority—are all involved. that determines how popular a standard curve is:

With A (E, P, S) = 1, Jerry generates P, E, and S, which are auxiliary data points and curves, respectively. Alice and Bob have confirmed that A(E, P, S) = 1.

1. Prior to sending aP, Alice creates a private integer a.
2. Bob creates a unique integer b and transmits it as bP.
3. The ath multiple of bP is used by Alice to calculate abP.
4. The bth multiple of aP is what Bob uses to calculate abP.
5. Alice and Bob use abP to generate an encryption key.

We take a look at what might happen if Jerry and Eve, an eavesdropper, worked together to decipher Alice and Bob's cryptography.

1. Vulnerabilities that are not publicly recognized may exist, such as ellipses E whose cE,P values are less than the maximum effective publicly disclosed assaults suggest. We begin with the premise that Jerry and Eve are in the dark about a security hole that affects a percentage c of publicly believed secure curves. Jerry should standardize a susceptible curve as his tactic.
2. For certain choices of A, there is a restriction on the number of curves E for which suitable supplemental data S is immediately accessible. Unless 1/c is much larger, it is not reasonable to assume that every vulnerable set (E, P, S) will have A (E, P, S) = 1. than this limit, as Jerry has pointed out. Luckily for Jerry, we prove that this restriction is far bigger than what the general population believes it to be.

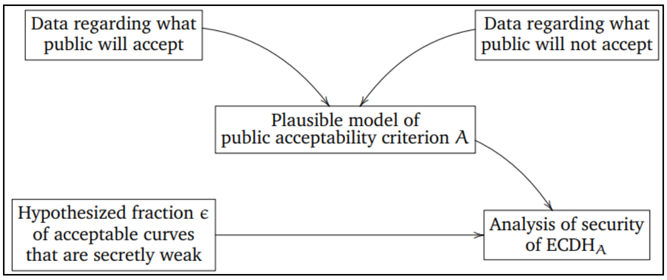

Fig 2: The flow of data in this article

Five distinct models of the public acceptability criteria R and five distinct forms of the auxiliary curve data S are used to stratify the available data on popular acceptance. For c, we examine the safety of each R.

1. Various choices of R complicate Jerry's task of finding a vulnerable (E, P, S) with R (E, P, S) = 1, even if these choices do not limit the number of vulnerable E for which S exists. To see the cost analysis of this calculation.

After Jerry finds a susceptible (E, P, S) such that R(E, P, S)=1, Eve could manage exploit it and read the encrypted data that Bob and Alice have sent.

Estimations of the likelihood of several possible assaults.

Here, we simulate Jerry's hidden weakness after a number of plausible public assaults. For every assault, we check whether it is likely to succeed against curves that weren't specifically selected to be resistant to it. For a c that Jerry is interested in, any such probability is a plausible assumption.

To find out how likely certain values are, one may use the prime-number theorem. of 4, but it becomes useless when the value of 4 falls below. In order to assess the issue

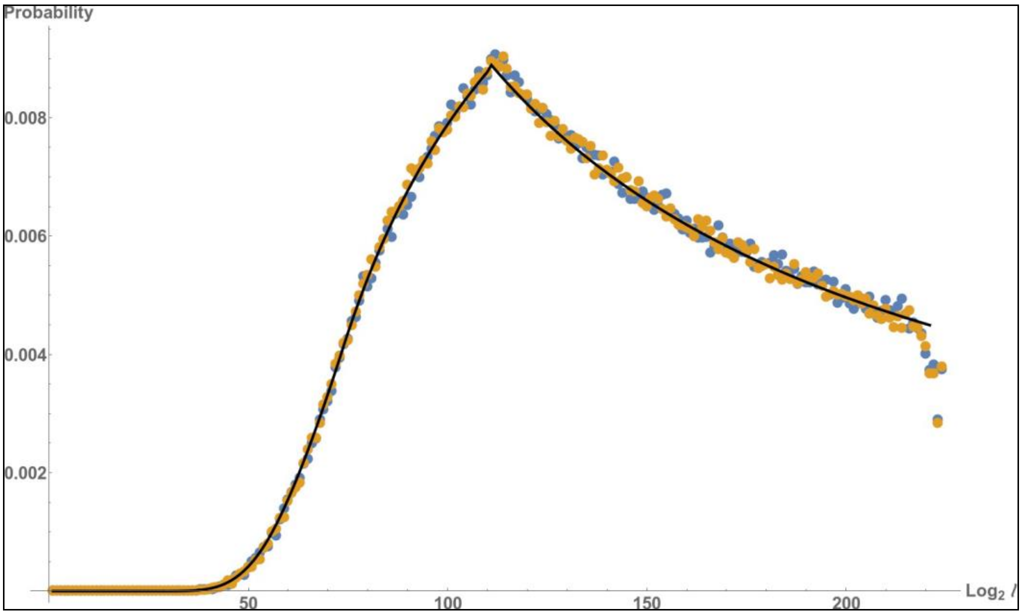

Fig 3: Largest prime factor vs the likelihood. The blue curves are regular. The curves' twists (E. *Orange*) For E. Black, there is the Dickman value. Since orange is superimposed on top of blue in the plot, it stands out more than blue

Capacity to use the following outcome from Dickman (for example, see [Gra08]). The term "y-smooth integers" is used to describe a set of integers ≤ x where the highest prime factor is no more than y. So, here is Dickman's outcome:

$\Psi(x, y) \sim x\rho(u)$ as $x \to$, where $x = y^u$.

In this case, the "Dickman ρ function" (ρ) meets $\rho(u) = 1$ for $0 \le u \le 1$ and $-u\rho'(u) = \rho(u - 1)$ for $u \ge 1$, ρ′ denotes the right derivative. Accurately computing ρ(u) is not a tough task.

We confirmed experimentally how effectively ℓ yet again, for the NIST P-224 prime, follows this conservative estimate. For every k, we estimated how many numbers in the Hasse interval had the biggest prime factor has exactly k bits: Ψ $(p+1 + 2^{\sqrt{p}}, 2^k) - \Psi (p+1 - 2^{\sqrt{p}}, 2^k) - \Psi (p+1 + 2^{\sqrt{p}}, 2^{k-1}) + \Psi(p+1 - 2^{\sqrt{p}}, 2^{k-1})$.

This was then split by $4^{\sqrt{p}}$ (the length of the Hasse interval) to get the graph shown in Figure 3, which is black in color. Figure 3 shows the blue dot for the proportion of curves with 4 having k bits and the orange dot for the fraction of curves with 4′ having k bits, which were likewise calculated empirically. Figure 3 's dots are positioned below the right end of the graph for the reasons that will be discussed. when r is less than 4 the estimate is quite close to the experimental data.

Only over 20% of 224-bit curves really $\ell < 2^{100}$, rendering the rho assault cost manageable, about 2^{50} functions that are elliptic in shape. Yet, when u grows, ρ(u) decreases at a fast pace. (it is roughly $1/u^u$), So, as the size of the curve rises, the likelihood of attaining this fair cost likewise decreases significantly. For curves with 256 bits, the probability is ρ(2.56). $0.12 \approx 2^{-3}$. With 384-bit curves, the probability is ρ (3.84) $\approx$ 0.0073 $\approx 2^{-7}$Assuming 512-bit curves, the probability is ρ (5.12) $\approx$ 0.00025 $\approx 2^{-12}$.

After discussing rho attacks on any curve, we go on to twist attacks on curves with a cofactor of 1. To accommodate 250 elliptic-curve twist attacks.

Table 1: Estimated probability that an elliptic curve modulo p has largest twist prime at most 2^2k plus the greatest twist prime by a considerable margin 2k, plus the greatest twist prime by a considerable margin 2k operations. In order to calculate the asymptotic semi smoothness probability, the estimates use the approach of [BP96].

p	k = 30	k = 40	k = 50	k = 60	k = 70	k = 80
P-224 prime	$2^{-15.74}$	$2^{-8.382}$	$2^{-4.752}$	$2^{-2.743}$	$2^{-1.560}$	$2^{-0.8601}$
P-256 prime	$2^{-20.47}$	$2^{-11.37}$	$2^{-6.730}$	$2^{-4.132}$	$2^{-2.551}$	$2^{-1.557}$
P-384 prime	$2^{-42.10}$	$2^{-25.51}$	$2^{-16.65}$	$2^{-11.37}$	$2^{-7.977}$	$2^{-5.708}$
P-521 prime	$2^{-68.64}$	$2^{-43.34}$	$2^{-29.57}$	$2^{-21.16}$	$2^{-15.63}$	$2^{-11.81}$

For example, according to [BL15] in general, the biggest prime The highest prime number that divides p+1 + t cannot exceed 2100, while the second-largest prime number that divides p + 1 + t cannot exceed 250. To rephrase, the equation p + 1 + t has to be (2100, 250)-semi smooth. As a refresher, to be (y, s)- semi smooth, an integer must have the highest prime number that divides p+1 + t cannot exceed 2100, while the second-largest prime number that divides p + 1 + t cannot exceed 250 factors less than y. Since it is difficult to batch that portion of the twist attack over several targets, even stricter constraints for the second-largest prime should be considered.

Our assessment of the likelihood of semi-smoothness was similar to that of rho attacks. To begin, for any integer p that is uniformly distributed throughout the Hasse interval, we may calculate the chance of semi smoothness as follows: p + 1 + t = ln(u(u)). To determine the semi-smoothness probability assuming a uniformly distributed integer, the following step is to use a two-variable extension of ρ that is known. Third, to determine this generalization, use the method suggested by Peralta and Bach [BP96]. The outcomes for 256-bit curves start at $2^{-6.730}$. and extend all the way up to $2^{-29.57}$ for curves with 521 bits. Results of comparable calculations for are shown in Table 1. different prime values and attainable attack cost constraints.

Conclusion

In conclusion, when confronted with curves that are not designed to resist credible attacks, there is a wide variety of success possibilities presented in the public literature for such attacks. The probability indicated earlier consist of 2^{-4}, 2^{-8}, 2^{-11}, 2^{-16}, and 2^{-25}. Since Jerry's covert attack may jeopardize a curve that satisfies public security norms, it's appropriate to consider a range of possibilities for c.

References

1. Dorostkar Z. Mathematics for Cryptography: A Guide to Mathematical Fundamentals of Different Classes of Cryptography Algorithms; c2023.
2. Wu H. General analysis on essential mathematical principles of elliptic curve cryptography. Theoretical and Natural Science. 2023;10:123-129. doi:10.54254/2753-8818/10/20230327.
3. Easttom W. Modern Cryptography: Applied Mathematics for Encryption and Information Security. 2021. doi:10.1007/978-3-030-63115-4.
4. Hamlin N. Number in Mathematical Cryptography. Open Journal of Discrete Mathematics. 2017;7:13-31. doi:10.4236/ojdm.2017.71003.
5. Selvam A, Padmalatha MS. A Study on Network Security and Cryptography; c2022.
6. Mavroeidis V, Kamer V, Zych MD, Jøsang A. The Impact of Quantum Computing on Present Cryptography. Int J Adv Comput Sci Appl. 2018;9(3):01-10.
7. Norman J. Formulation of Shor's Algorithm for Quantum Computers. April 30, 2020. Accessed June 13, 2020. Available from: http://www.historyofinformation.com/detail.php?id=3877
8. Buchmann J, Braun J, Demirel D, Geihs M. Quantum cryptography: a view from classical cryptography. Quantum Sci Technol. 2017;2(2):020502.
9. Diffie W, Hellman ME. Privacy and Authentication: An Introduction to Cryptography. Proc IEEE. 1979;67(3):397-427.
10. Li T, Yin ZQ. Quantum superposition, entanglement, and state teleportation of a microorganism on an electromechanical oscillator. Sci Bull. 2016;61(2):163-71.
11. Yoloğlu N. Yakinsama (Convergence) Ve Çapraz Medya (Crossmedia) Stratejisinin Medya Sektöründe Yansimalari. Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi. 2019;7(3):1449-64.