Enhancing Mobile Security with Elliptic Curve Cryptography (ECC)

By: Daniel Appel

Cal Poly Pomona, Computer Science Department - Cal Poly Pomona Cybersecurity and Awareness Fair 2024

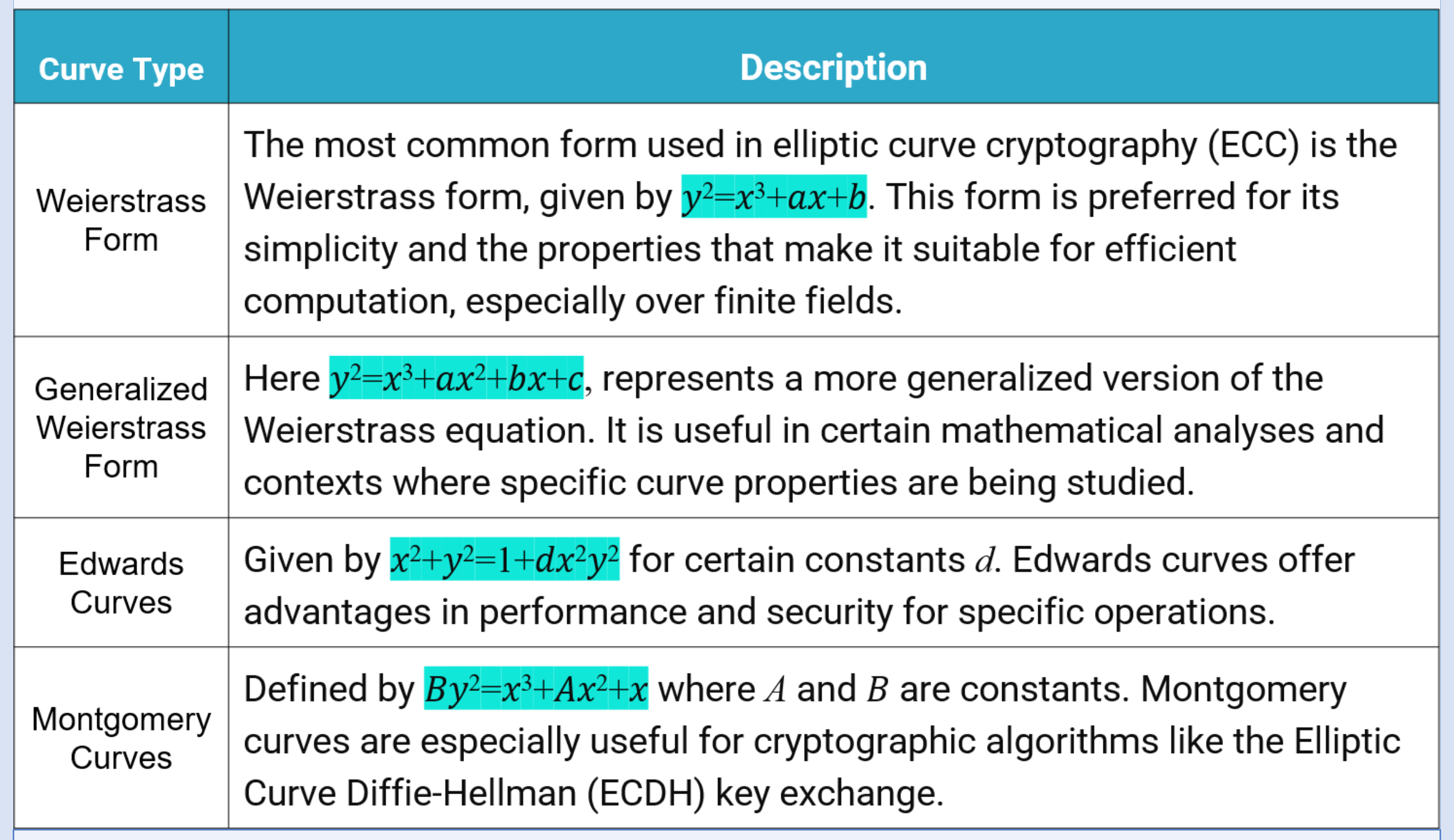
INTRODUCTION

Purpose:

- The purpose of this study is to explore the application of Elliptic Curve Cryptography (ECC) and its different forms, such as Hyper ECC and Supersingular Elliptical Curves (SECC), in enhancing mobile security.
- ECC is gaining prominence due to its ability to provide the same level of security as other cryptographic systems but with significantly smaller key sizes, making it particularly suited for mobile devices.

OBJECTIVES

1) Review of ECC's Mathematical Foundations and Properties.
2) Utilization of ECC's Cryptographic Principles in Mobile Security.
3) Examination of the Discrete Logarithm Problem and SECC's Approach:



Curve Type	Description
Weierstrass Form	The most common form used in elliptic curve cryptography (ECC) is the Weierstrass form, given by $y^2=x^3+ax+b$. This form is preferred for its simplicity and the properties that make it suitable for efficient computation, especially over finite fields.
Generalized Weierstrass Form	Here $y^2=x^3+ax^2+bx+c$, represents a more generalized version of the Weierstrass equation. It is useful in certain mathematical analyses and contexts where specific curve properties are being studied.
Edwards Curves	Given by $x^2+y^2=1+dx^2y^2$ for certain constants d. Edwards curves offer advantages in performance and security for specific operations.
Montgomery Curves	Defined by $By^2=x^3+Ax^2+x$ where A and B are constants. Montgomery curves are especially useful for cryptographic algorithms like the Elliptic Curve Diffie-Hellman (ECDH) key exchange.

Figure 1: ECC Forms

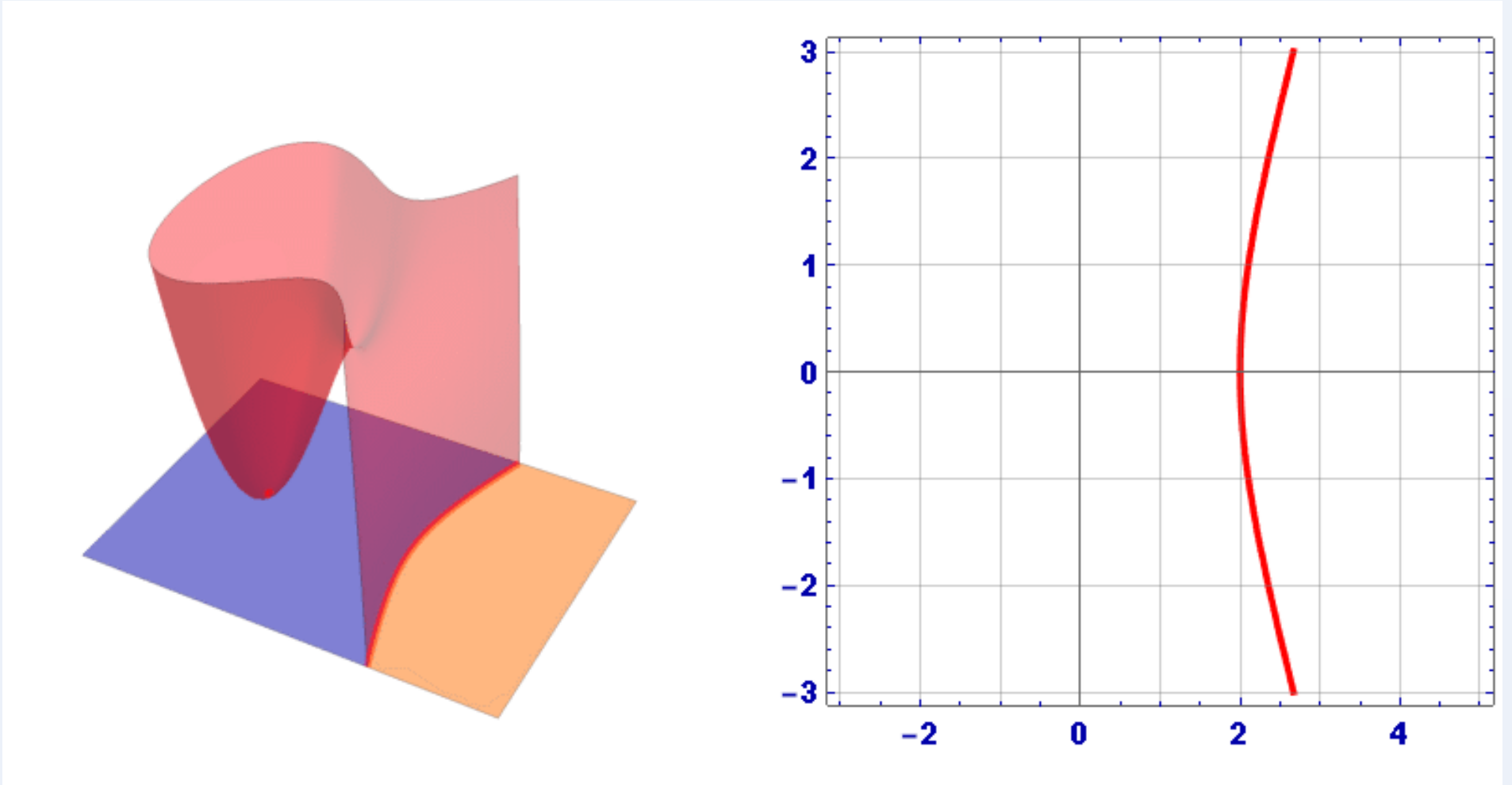


Figure 2: ECC 3D Model

Source: https://www.allaboutcircuits.com/technical-articles/elliptic-curve-cryptography-in-embedded-systems/

METHODS

- **Weierstrass Form**: ECC is primarily based on the mathematical structure of elliptic curves. The standard Weierstrass equation, $y^2=x^3+ax+b$, defines the curve, where 'a' and 'b' are constants that determine the shape and properties of the curve. This form is widely used because of its simplicity and the efficiency it provides in computation, making it suitable for cryptographic applications.
- **Hyper ECC Application**: Hyper Elliptic Curve Cryptography (Hyper ECC) extends ECC by using curves of higher genus (greater complexity), providing even more compact key sizes and potentially greater security. It uses higher-order polynomials to define the curve, allowing for a more intricate and secure cryptographic system, especially for resource-constrained environments like mobile devices.
- **Public Key Cryptography**: ECC operates on the principles of public key cryptography, where a pair of keys (public and private) are generated based on elliptic curve mathematics. The public key can be distributed openly, while the private key remains confidential. The security of ECC lies in the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is computationally infeasible to break with current technologies.
- **Discrete Logarithm Problem**: ECC's security is underpinned by the ECDLP, which involves finding a scalar multiplier given two points on the elliptic curve, a task that is computationally difficult. This complexity forms the core of ECC's resistance to attacks.

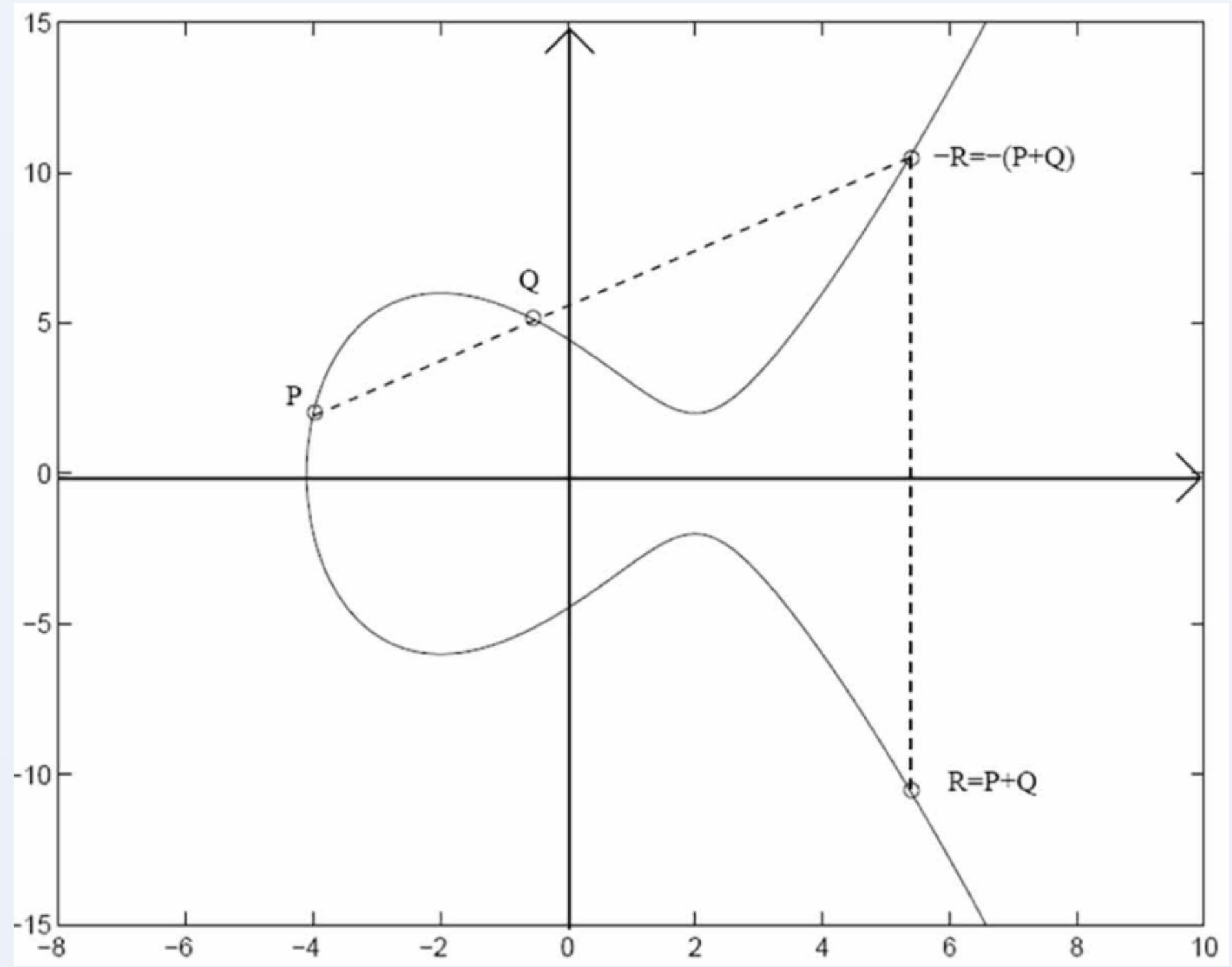


Figure 3: ECC Point Addition

Source: https://link.springer.com/article/10.1007/s11227-023-05789-w

RESULTS

- Findings suggest ECC's smaller key sizes result in reduced computational load, which is critical for mobile devices with limited processing power and battery life.
- Hyper ECC can be seen as a stronger alternative to standard ECC, while SSEC is highlighted as a post-quantum option.
- Applications include secure messaging, digital signatures, and authentication, providing solid solutions for secure communications and transactions.
- Supersingular Elliptic Curves (SSEC) in Quantum Context: As quantum computing advances, traditional ECC might become vulnerable due to quantum algorithms like Shor's algorithm. SSEC offers a potential solution, being more resistant to quantum attacks. These curves utilize isogenies between supersingular elliptic curves, creating a complex structure that current quantum algorithms cannot efficiently solve, positioning SECC as an ideal candidate for post-quantum cryptography.

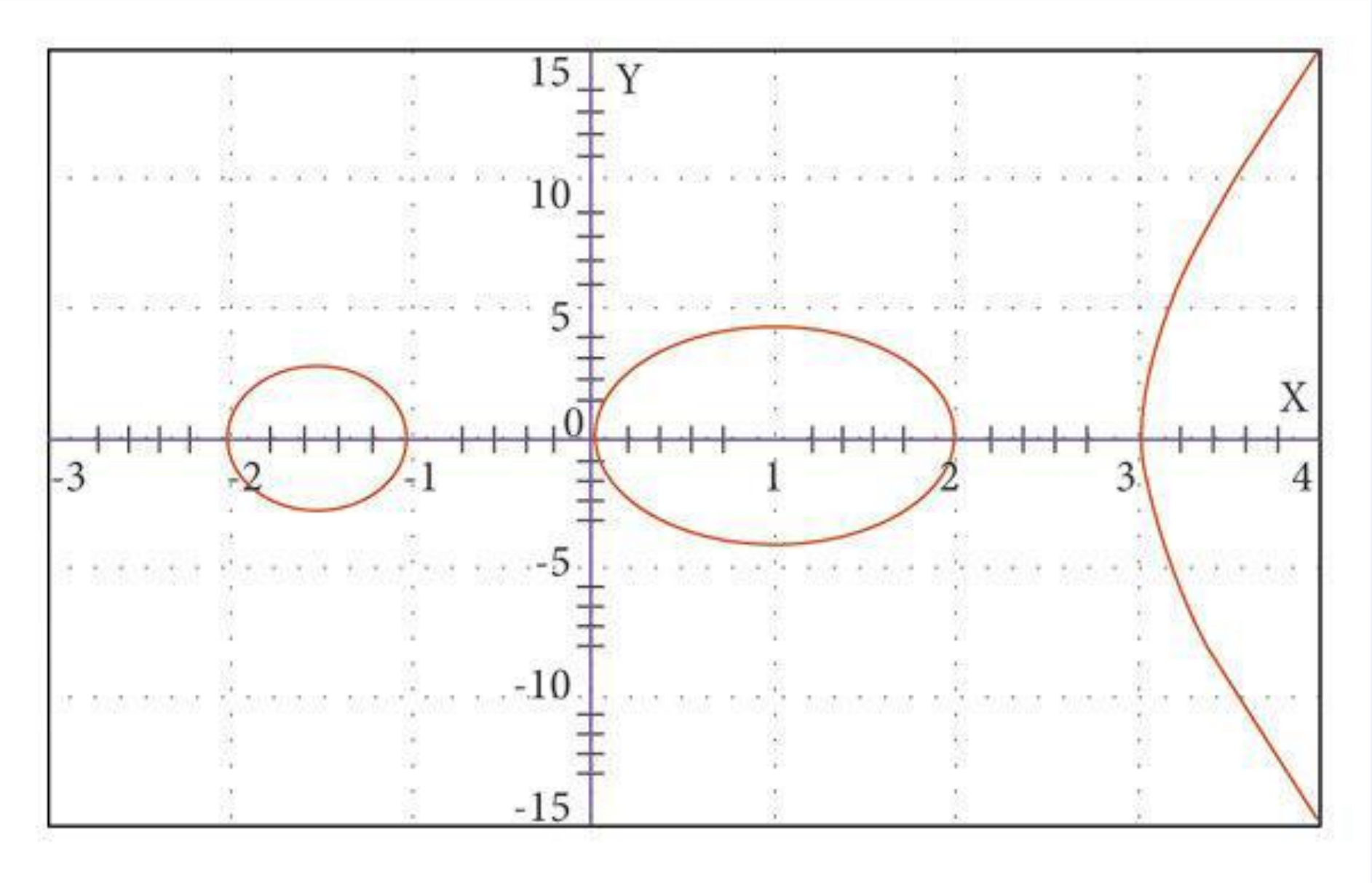


Figure 4: Hyper ECC

Source: https://shorturl.at/jybDq

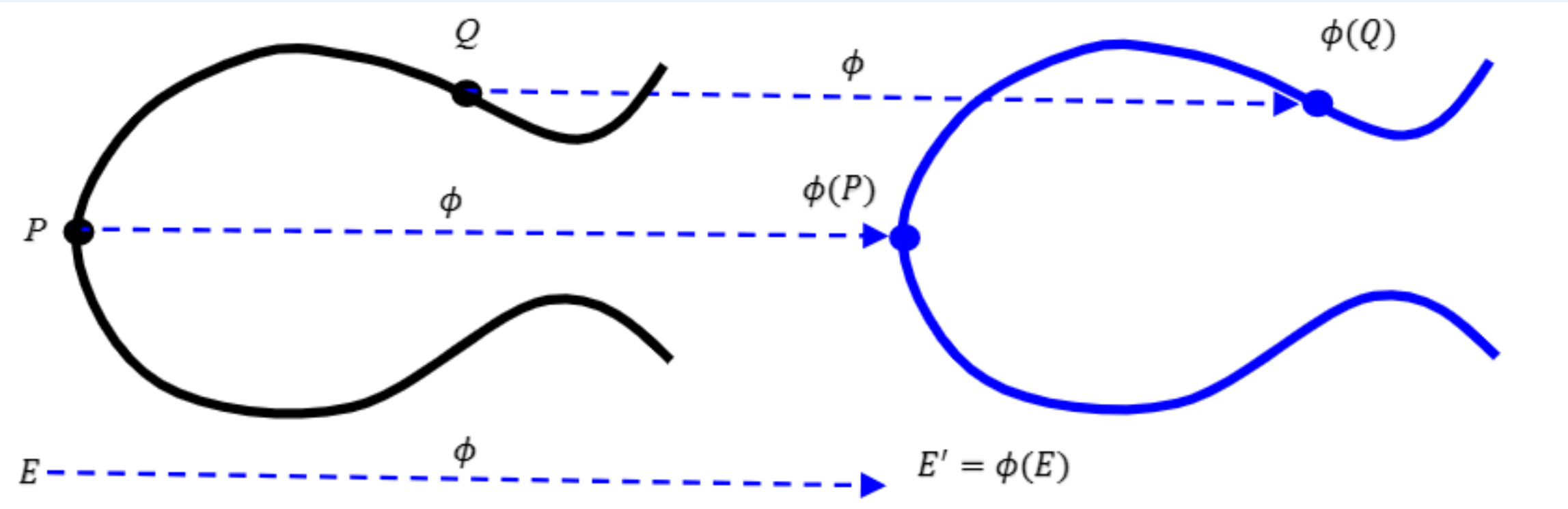
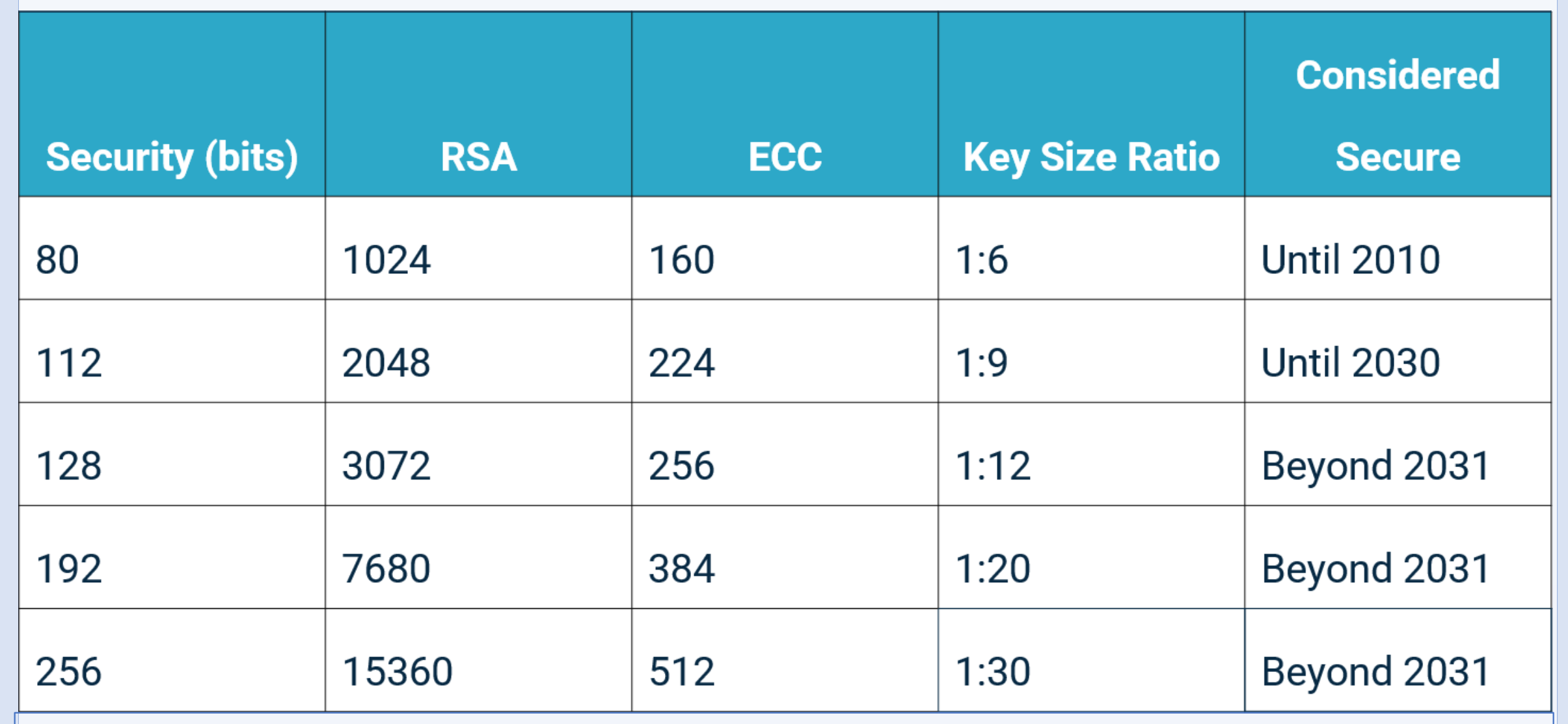


Figure 5: Supersingular ECC with Isogeny-Based Cryptography

Source: https://shorturl.at/UDR5l

CONCLUSIONS

- ECC and its variations offer substantial benefits over traditional encryption methods like RSA, particularly in mobile security contexts.
- Its efficiency and smaller key size make ECC ideal for resource-constrained environments like smartphones.
- Future developments, such as quantum-resistant algorithms, will further enhance ECC's potential in securing mobile platforms.



Security (bits)	RSA	ECC	Key Size Ratio	Considered Secure
80	1024	160	1:6	Until 2010
112	2048	224	1:9	Until 2030
128	3072	256	1:12	Beyond 2031
192	7680	384	1:20	Beyond 2031
256	15360	512	1:30	Beyond 2031

Figure 6: Rivest-Shamir-Adleman (RSA) and ECC Comparison

References

1) All About Circuits. (n.d.). *Elliptic Curve Cryptography in Embedded Systems*. https://www.allaboutcircuits.com/technical-articles/elliptic-curve-cryptography-in-embedded-systems/
2) Avi Networks. (n.d.). *Elliptic Curve Cryptography*. https://avinetworks.com/glossary/elliptic-curve-cryptography/
3) Boot.dev. (n.d.). *A Relatively Easy to Understand Primer on Elliptic Curve Cryptography*. Retrieved from https://blog.boot.dev/cryptography/elliptic-curve-cryptography/
4) Cheap SSL Security. (n.d.). *ECC vs RSA: Comparing SSL/TLS Algorithms.* https://cheapsslsecurity.com/p/ecc-vs-rsa-comparing-ssl-tls-algorithms
5) Cloudflare. (n.d.). *A Relatively Easy to Understand Primer on Elliptic Curve Cryptography*. https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/
6) Daisie. (n.d.). *Elliptic Curve Cryptography: In-Depth Guide*. https://blog.daisie.com/elliptic-curve-cryptography-in-depth-guide/
7) IJSER. (n.d.). *Overview of History of Elliptic Curves and Its Use in Cryptography* https://www.ijser.org/researchpaper/Overview-of-History-of-Elliptic-Curves-and-its-use-in-cryptography.pdf
8) ISACA. (2016). *Can Elliptic Curve Cryptography Be Trusted? A Brief Analysis of the Security of a Popular Cryptosystem*. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/can-elliptic-curve-cryptography-be-trusted-a-brief-analysis-of-the-security-of-a-popular-cryptosyste
9) Maimuţ, Diana, and Alexandru Cristian Matei. "Speeding-up Elliptic Curve Cryptography Algorithms." *MDPI*, Multidisciplinary Digital Publishing Institute, 7 Oct. 2022, www.mdpi.com/2227-7390/10/19/3676.
10) SSL2Buy. (n.d.). *RSA vs ECC: Which is Better Algorithm for Security?* https://www.ssl2buy.com/wiki/rsa-vs-ecc-which-is-better-algorithm-for-security
11) Ullah, Shamsher, et al. "Elliptic Curve Cryptography; Applications, Challenges, Recent Advances, and Future Trends: A Comprehensive Survey." *Science Direct*, Elsevier, 23 Dec. 2022, www.sciencedirect.com/science/article/abs/pii/S1574013722000648.
12) TechTarget. (n.d.). *Elliptical Curve Cryptography*. https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography
13) University of Chicago. (n.d.). *Shevchuk*, A. (2020). https://math.uchicago.edu/~may/REU2020/REUPapers/Shevchuk.pdf
14) Wohlwend, Jeremy. *Elliptic Curve Cryptography: Properties and Applications*. 2016, MIT, math.mit.edu/~apost/courses/18.204-2016/18.204_Jeremy_Wohlwend_final_paper.pdf.