Security in relation to key length and Cryptographical Methods

Joseph Patrick C. Galvez

American Military University

ISCC266: Cryptography Concepts

Mr. Joel Stewart

5/25/2025

Security in relation to key length and Cryptographical Methods

A relatively new cryptographic method was created with the advantage of efficiency in regards to both computing power and security, this new method is also able to achieve a similar or better level of security with a much smaller key size compared to its predecessors. This new cryptographic method is called ECC or Elliptic Curve Cryptography. The difference between ECC and its counterparts is that ECC uses an elliptic curve in its mathematical calculations instead of just substitution and permutation like in AES and RSA. In addition to this ECC also achieves a higher level of security with a smaller key size compared to RSA and AES.

In mathematics an elliptical curve is any curve that is symmetric about the x axis (although it does not have to be on the x axis), another characteristic is that any straight line drawn through one will result in no more than three intersections with the curve. ECC uses a finite elliptic curve which are either the curves p-256 or p-384 (Polk et al., 2015, p.5) as the basis of its operation. Its operation takes the form of the elliptic curve discrete logarithm problem which uses the quality of the elliptic curve which has no more than three intersections with a straight line drawn through it. Points a, b, and c are both in this line, point d will be reflected across the x axis directly below, a line can be drawn from point a to point d which will result in another intersect which is point e (Paar & Pelzl, 2010, p.242). To crack the encryption the problem P & Q =kP, find scalar k must be solved, this problem is exponentially difficult. This demonstrates how the symmetry of the elliptic curve is used to easily produce new points in a way that is computationally more efficient when it comes to the encryption process.

The security of ECC comes from the fact that the number of times a new point is plotted is the private key. Now you may think that all of the values will take on the geometry of the curve and be easily predictable but modulo and the finite key takes care of that because this two put together will make the points appear to be scattered randomly which adds greatly to its security by making it difficult to find the original value the addition of modulo in ECC is defined in Paar and Plezl (2010) in definition 9.1.1. In conclusion ECC uses a predefined elliptical curve as a scaffold for the sake of computational efficiency and the addition of modulo enhances its security by making it exceedingly difficult to find both the number of times the point was doubled or where the starting point even was.

In conclusion, ECC was implemented to meet the threat posed by increasing levels of computational capacity while meeting the needs of computational efficiency in regard to encryption.

ECC meets the first criteria by using the structure of the elliptic curve to plot points by reflections and intersections from the starting point to the new state, this process uses predefined curves defined by the NIST for the sake of standardization. ECC also meets the second criteria by utilizing the elliptic curve discrete logarithm problem which gets exponentially harder the longer the key is.

The first section of your paper is your introduction. Use these paragraphs to provide background and context. “Introduction” should not be used as a section heading as it’s assumed your paper will begin with an introduction. Remember to use first-person tense. Anytime you want to start a section on a new page, instead of adding page breaks, use the **Section Title** style. (To see the reader’s view of your document, click on the **View** tabthen select **Reading View.**)

The body of your paper should be indented one half-inch on the first line of each new paragraph and double-spaced. When introducing key terms, use *Italics* to highlight the term in its first use, only. APA Style provides for up to five heading levels, shown in the paragraphs that follow. Note that all text styles for this template are available on the **Home**tab of the ribbon, in the **Styles** gallery.

References

Polk, T., Dodson, D., Burr, W., Ferraiolo, H., & Cooper, D. (2015). *Cryptographic algorithms and key sizes for personal identity verification* (NIST Special Publication 800-78-4). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-78-4>

Paar, C., & Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Springer. <https://doi.org/10.1007/978-3-642-04101-3>

*For additional information on APA Style formatting, please consult the* [*APA Style Manual, 7th*](https://apastyle.apa.org/style-grammar-guidelines) *Edition.*