Bellevue University

Elliptic Curve Cryptography

Timothy Jelinek

CIS313-T301 Cryptography

10/15/2023

Elliptic Curve Cryptography is an asymmetric authentication. Asymmetric cryptography is when there is a pair of keys that are generated. The keys generated are a public key and a private key.

Elliptic Curve Cryptography is most notably used for digital signatures in cryptocurrencies. The two significant cryptocurrencies that use Elliptic Curve Cryptography are Bitcoin and Ethereum when they sign transactions.

Elliptic Curve Cryptography has advantages over its counterparts, such as requiring less power to generate keys and smaller keys that are just as secure as RSA's. Elliptic Curve Cryptography is known to be more secure because it is more challenging to solve elliptic curves because of an added level of protection. Finally, Elliptic Curve Cryptography is faster than other algorithms, so it is a better choice for applications that require fast encryption and decryption.

Elliptic Curve Cryptography is known for having vulnerabilities like getting side-channel attacks and twist-security attacks. These attacks result in information leaks.

An application that uses Elliptic Curve Cryptography is Keeper's Enterprise Password Manager. This app is a password management tool that helps you keep your passwords safe and stored. Keeper's encryption model documentation compares the strength of 256-bit elliptic curves against password-derived key vaults. Keeper uses a Single Sign-On, so you don't need a master password. This is safe as attackers find it harder to get through this login method than just obtaining a password. Some Single Sign-Ons have two-factor authentication to make sure you are the person trying to log in to your account.

Source:

"Asymmetric Cryptography (Public Key Cryptography)" Brush, https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography?Offer=abMeterCharCount_var2. Accessed 15 October 2023.

"Elliptic Curve Cryptography" Avinetworks, https://avinetworks.com/glossary/elliptic-curve-cryptography/#:~:text=Elliptic%20Curve%20Cryptography%20(ECC)%20is,and%20encryption%20of%20web%20traffic. Accessed 15 October 2023.

"Keeper – The Only Enterprise Password Manager to use Elliptic Curve Cryptography," Julienne, https://www.keepersecurity.com/blog/2023/03/24/keeper-the-only-enterprise-password-manager-to-use-elliptic-curve-cryptography/#:~:text=Keeper's%20Enterprise%20Password%20Manager%20is,the%20mathematics%20of%20elliptic%20curves. Accessed 15 October 2023.