Point Validation in Elliptic Curve Cryptography

1 Abstract

Point validation is a crucial step in elliptic curve cryptography (ECC) that ensures that the points used in cryptographic operations belong to the specified curve. Failure to perform point validation can lead to serious security vulnerabilities such as invalid curve attacks, small subgroup attacks, twist attacks, or signature malleability attacks. In this report, we present the importance of point validation for the Muon protocol implementation, which relies on ECC for security. We also demonstrate how point validation can be easily integrated into the existing Muon protocol functions. We are pleased to announce that the current implementation of the Muon protocol includes elliptic curve point validation.

2 Importance of Point Validation in cryptography

Point validation is crucial in preventing invalid curve attacks, where an attacker sends a point that does not belong to the intended curve but to another curve with weaker security properties. For example, if an attacker sends a point on a twist of the original curve, they may be able to solve the discrete logarithm problem on that twist and recover some information about the private key of a legitimate user. This can compromise protocols such as ECDH or ECDSA that rely on elliptic curves. Point validation also avoids interoperability issues that can arise from different representations or encodings of elliptic curve points.

3 How to Perform Elliptic Curve Point Validation

To perform point validation on an elliptic curve, four checks must be done for each point:

1. Check that the coordinates are lower than the field modulus. For example, if the field modulus is a prime number p, then the x and y coordinates of each point must be in the range [0, p-1]. This check ensures that the point is within the finite field defined by the modulus.
2. Check that the coordinates satisfy the curve equation. Each point must satisfy the elliptic curve equation, which is y^2 = x^3 + ax + b, where a and b are constants that define the curve. For example, a valid point on the elliptic curve defined by y^2 = x^3 + 3x + 1 in GF(7) is (2,1) because (1)^2 = (2)^3 + 3*(2) + 1 (mod 7). However, a point (3,4) is not valid because (4)^2 ≠ (3)^3 + 3*(3) + 1 (mod 7). This check ensures that the point lies on the intended curve.
3. Check that the point is not the point at infinity. The point at infinity is the identity element of the elliptic curve group and has no defined x and y coordinates. This check ensures that the point is not a special case that can be used to attack the cryptographic protocol.

4. Check that the point belongs to the correct subgroup. Elliptic curve groups have different subgroups, each with its own security properties. The point must belong to the subgroup that is suitable for the cryptographic protocol. For example, some protocols require the use of points in a subgroup of prime order, while others require the use of points in a subgroup of composite order. This check ensures that the point is compatible with the cryptographic protocol.

To perform the checks, the coordinates of the point are substituted into the curve equation, and the results are computed modulo the field modulus. If all the checks pass, the point is considered valid. If any of the checks fail, the point is considered invalid, and it should be rejected.

4 Integrating Elliptic Curve Point Validation into Muon Protocol

We recognized the importance of point validation and immediately integrated this feature into the Muon protocol. The current implementation of Muon protocol includes elliptic curve point validation, ensuring that all points used in cryptographic operations belong to the intended curve. This integration mitigates the potential security risks associated with invalid curve attacks and other ECC-related vulnerabilities.

To perform elliptic curve point validation, we checked that the coordinates of each point correspond to a valid curve point by verifying that they satisfy the equation of the elliptic curve. By performing this check, we can ensure that the points used in cryptographic operations are valid and belong to the intended curve.

5 Conclusion

In conclusion, we recognize the importance of point validation in ECC and its critical role in ensuring the security of the Muon protocol. By integrating elliptic curve point validation into the Muon protocol, we have mitigated potential security risks and ensured that all points used in cryptographic operations belong to the intended curve.

6 References

[1] Kalra, Sheetal, and Sandeep K. Sood. "Elliptic curve cryptography: Current status and research challenges." In High Performance Architecture and Grid Computing: International Conference, HPAGC 2011, Chandigarh, India, July 19-20, 2011. Proceedings, pp. 455-460. Springer Berlin Heidelberg, 2011.

[2] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 2018.

[3] Chen, Lily, Dustin Moody, Karen Randall, Andrew Regenscheid, and Angela Robinson. "Recommendations for discrete logarithm-based cryptography: Elliptic curve domain parameters." (2023).