ÇOK DEĞIŞKENLI POLINOM TABANLI KRIPTOGRAFI

Talha Arıkan[1], Mustafa Solmaz[2*],

[1] *Hacettepe Üniversitesi, Fen Fakültesi, Matematik Bölümü, Ankara, Tükiye*
[2] *Hacettepe Üniversitesi, Fen Fakültesi, Matematik Bölümü, Ankara, Türkiye*

ÖZET

Shor Algoritması ile birlikte kuantum hesaplama gücüne sahip cihazlarda günümüz asimetrik kriptografisinin altında yatan çarpanlara ayırma ve ayrık logaritma problemlerinin çok daha hızlı çözülebileceği gerçeğinden hareketle kuantum sonrası kriptografi araştırmaları her geçen gün hız kazanmaktadır. Güvenliliğini çok değişkenli polinom sistemlerinin çözümünün zorluğuna dayandıran, çok değişkenli polinom tabanlı sistemler altında yatan ve kuantum cihazlara karşı dayanıklı olan MQ-Problem ile kuantum-sonrası kriptografi araştırmalarında önemli bir yer tutmaktadır. Bu bildiride çok değişkenli polinom tabanlı sistemlerden günümüzde güncelliğini koruyarak devam eden ve hala standartizasyon yarışmalarında önemli bir yer tutan UOV (Unbalanced Oil and Vinegar) ve modern bir UOV varyasyonu olan MAYO algoritmaları tanıtılacaktır.

***A*nahtar Kelimeler** Kuantum Sonrası Kriptografi, Kriptografi,Dijital İmza

Kaynaklar

[1] A. Kipnis, J.-J. Patarin, L. Goubin, *Unbalanced Oil and Vinegar Signature Schemes* , Advances in Cryptology (EUROCRYPT 1999). Lecture Notes in Computer Science, vol. 1592

[2] W.Beullens, *MAYO: Practical Post-Quantum Signitures from Oil-and-Vinegar Maps*, Selected Areas in Cryptography (SAC 2021)

[3] W.Beullens et al., *UOV: Unbalanced Oil and Vinegar (Algorithm Specifications and Supporting Documentation Version 2.0)*,NIST, Standardization of Additional Digital Signature Schemes (2025) .

[*] *mustafa.solmaz@hacettepe.edu.tr*