HACETTEPE ÜNİVERSİTESİ

25 Haziran, 2025
Çarşamba
14:00

Hacettepe Üniversitesi
Matematik Bölümü
Yaşar Ataman Salonu

MATEMATİK BÖLÜMÜ

GENEL **SEMİNER**

KONUŞMACI

Orhun Kara
İzmir Yüksek Teknoloji Enstitüsü, Türkiye

BAŞLIK

AES Şifreleme Algoritmasının Farksal Kriptoanalize Karşı Güvenliği

ÖZET

AES birçok kriptografik protokolde ve uygulamada gizliliği sağlamak için kullanılan oldukça yaygın bir blok şifreleme algoritmasıdır. AES'in özellikle farksal saldırılara karşı güvenliğini sağlamak için tasarımcıları tarafından benimsenen güvenlik ölçütlerinden ve önlemlerden bahsedilecektir. Ayrıca AES'e yapılan imkansız farksal ve budanmış farksal saldırılar ile ilgili son yapılan çalışmalar anlatılacaktır.