IMPACT: International Journal of Research in Engineering and Technology
ISSN (P): 2347–4599; ISSN (E): 2321–8843
Vol. 12, Issue 10, Oct 2024, 1–10

EKR CRYPTOSYSTEM RESISTANCE AGAINST TO SIMPLE POWER ANALYSIS ATTACKS

Dr. E. Kesavulu Reddy

Professor, Department of Computer Science, S.V. University, Tirupati-Andhra Pradesh, India

Received: 09 Oct 2024 **Accepted:** 15 Oct 2024 **Published:** 20 Oct 2024

ABSTRACT

Elliptic curve cryptosystems are more efficient and secure than the conventional cryptosystems like RSA cryptosystems. We developed a Secret Key in the EKR Modified Montgomery Inversion Algorithm to eliminate the number of Iterations of the main loop directly leaks the value of f and also the attacker can not guess the Secret key (t) to retrieve the valuable information in smart cards and mobile devices. We want to develop the new cryptosystem based on EKR Modified Montgomery Inversion Algorithm to resistance against Simple Power Analysis Attacks in Side- channel Attacks in Elliptic Curve Cryptosystems like RSA Cryptosystems

KEYWORDS: *EKR modified Montgomery Inversion, E. Kesavulu Reddy Cryptosystems, RSA Cryptosystems*