Efficiency of the RDVFS countermeasure

S.Ordas, M.Carbonne, G.Ducharme, S.Tiran, P.Maurine

Abstract—The use of Dynamic Voltage and Frequency Scaling technique (DVFS) in Systems-on-Chip is becoming more and more common. This technique, re-named RDVFS for the occasion, has recently been proposed as a countermeasure against Side Channel Attacks (SCA) through the randomization of the choices of V and F, at the expense of power consumption. In this paper, theoretical and practical assessments of the robustness of the RDVFS countermeasure against CPA is proposed.