# Cryptology ePrint Archive: Report 2011/236

**Using Templates to Distinguish Multiplications from Squaring Operations**

*Neil Hanley and Michael Tunstall and William P. Marnane*

**Abstract:** Since side channel analysis was introduced as a method to recover secret information from an otherwise secure cryptosystem, many countermeasures have been proposed to prevent leakage from secure devices. Among these countermeasures is side channel atomicity that makes operations indistinguishable using side channel analysis. In this paper we present practical results of an attack on RSA signature generation, protected in this manner, based on the expected difference in Hamming weight between the result of a multiplication and a squaring operation. This work presents the first attack that we are aware of where template analysis can be used without requiring an open device to characterize an implementation of a given cryptographic algorithm. Moreover, an attacker does not need to know the plaintexts being operated on and, therefore, blinding and padding countermeasures applied to the plaintext do not hinder the attack in any way.

**Category / Keywords:** Side Channel Analysis, template attack, RSA

**Publication Info:** An extended version will appear in Springer's International Journal of Information Security Infoma

**Date:** received 12 May 2011

**Contact author:** tunstall at cs bris ac uk