

6 to 9 September 2015 at the Arabella Hotel & Spa in the heart of the Kogelberg Biosphere Reserve near Hermanus, Western Cape, South Africa

# **An Investigation into the Signals Leakage From a Smartcard based on Different Runtime Code**

Ibraheem Frieslaar\*†, Barry Irwin †

\*Modelling and Digital Science, Council for Scientific and Industrial Research, Pretoria, South Africa.

<sup>1</sup> ifrieslaar@csir.co.za

†Department of Computer Science, Rhodes University, Grahamstown, South Africa.

<sup>2</sup> [b.irwin@ru.ac.za](mailto:b.irwin@ru.ac.za)

## **Abstract**

This paper investigates the power leakage of a smartcard. It is intended to answer two vital questions: what information is leaked out when different characters are used as output; and does the length of the output affect the amount of the information leaked. The investigation determines that as the length of the output is increased more bus lines are switched from a precharge state to a high state. This is related to the output array in the code increasing its length. Furthermore, this work shows that the output for different characters generates a different pattern. This is due to the fact that various characters needs different amount of bytes to be executed since they have different binary value. Additionally, the information leaked out can be directly linked to the smartcard's interpreter.