Asynchrobatic Circuit Techniques for Smartcard Applications

In VLSI systems, asynchronous techniques are known to have the potential to achieve low-power operation as well as average-case performance. Similarly, adiabatic circuit techniques have also been shown to make possible ultra-low-power computation. Recent work in the Department has combined these techniques in a design style labelled ‘asynchrobatic’ logic [1]. This work presented some implementations to established proof-of-concept and identified several promising application areas. One such area is very-wide data-path processors which benefit heavily from the technique because overheads of the design style are amortized [2].

Smartcards, particularly contact-less smartcards, require low-power operation. They also typically use very-wide data-paths particularly for the implementation of on-chip cryptographic algorithms. Smartcards also need to be resistant to attacks aimed at revealing or manipulating secure, on-chip data. Conventional cryptographic implementations can be vulnerable to such attacks especially through analysis of their supply currents. Adiabatic and quasi-adiabatic circuits have very slowly changing power supply currents which makes attack by supply current analysis particularly difficult.

Therefore these two properties, ultra-low-power and resistance to attack, recommend asynchrobatic circuits for smartcard implementations and make this a particularly promising application area in which to exploit and quantify their benefits. If this approach proves effective, it would find use in future generations of smartcard products.

Bibliography
