論文の内容の要旨

Dual Pipeline Self Synchronous Circuits for High Performance, Energy Minimum, and Error Robust Operation

（耐誤動作特性を有する低電力・高性能二重パイプライン型自己同期回路）

氏名　ベンジャミン　ステファン　デブリン

In this thesis we propose the use of dual pipeline self synchronous circuits in order to address the ever increasing VLSI problem of large uncontrollable variation, while still being able to achieve *high performance*, *energy minimum*, and *error robust operation*. We present several circuit optimizations and both self synchronous field programmable gate arrays (SSFPGA) and application-specific self synchronous RSA (SSRSA) crypto engine designs. Designs are proven with multiple silicon implementations in 65nm CMOS and 40nm CMOS, showing the real-world feasibility and advantages gained by using dual pipeline self synchronous circuits.

Chapter 1 introduces the motivation for this research - variation, which is ever increasing as VLSI technology shrinks and supply voltages decrease, and its impact on very large scale integration (VLSI) systems. We then explain the difference between synchronous and asynchronous operation, and the advantages that can be gained by using an asynchronous delay-insensitive architecture over one that is timing constrained by a global synchronous clock. There are many circuit styles within asynchronous technology, and so we further explain how self synchronous operation fits into the asynchronous model. Related work is then reviewed.

Chapter 2 introduces the dual pipeline self synchronous circuit style used in this thesis. Dual-rail signaling and bit-level completion detection circuits with fine grained gate-level pipeline stages are used to achieve the most robust operation possible within the asynchronous model, while maintaining high performance due to dual pipelines which conceal the differential cascode voltage swing logic (DCVSL) precharging time. The various basic circuit blocks required to design a self synchronous system are explained.

Chapter 3 describes several circuit optimizations with analysis, leading to a range of different circuits that use modifications to self synchronous technology, designed to be able to achieve different goals depending on the target application. Low voltage operation is first

targeted. In this region variation-induced delay uncertainty and leakage currents start to dominate operation, so we optimize keeper circuits that are robust to current races, introduce a low-overhead autonomous power gating scheme that can operate with gate-level granularity, and a show technique that can be used on individual gate-level pipelines in order to offset process variation. Next robust operation is targeted. We analyze self synchronous circuits in soft error prone environments, showing that this style of circuits is completely self checking for errors. A self synchronous watchdog circuit optimization is proposed which allows for autonomous detection, and correction of errors. We show that the dual pipelines can not only be used for performance increase but also as autonomous redundancy, with a circuit optimization that automatically disables faulty pipelines. Finally various error robustness techniques are compared.

Chapter 4 introduces the first real application of dual pipeline self synchronous circuit - a uniform logic SSFPGA. A split decoder-tree self synchronous lookup table is designed with fine grain pipelining in the routing blocks, and single buffer drivers for high performance. Fabrication results in 65nm CMOS show an operation range of 1.8V to 0.72V, with 3GHz throughput at the nominal 1.2V - the fastest presented in the state-of-the-art. To achieve energy minimum operation the autonomous power gating circuits described in Chapter 3 are utilized in a power-gated SSFPGA, which reduce leakage current even during maximum-throughput, and allowing for 7.2x energy savings at nominal 1.2V, and energy minimum operation of 27 fJ/operation 264MHz throughput at 0.6V. Operation range was extended to 0.37V. Finally we show error robust operations by using watchdog circuits in an error robust SSFPGA in 65nm CMOS. Robustness to power supply noise is extended to 83% at 1.2V, and 40% at 0.4V. Autonomously disabling faulty pipeline stages is shown in 40nm CMOS, and measurement results show correct error detection and disabling of pipeline stages.

Chapter 5 introduces an application specific implementation - a SSRSA crypto engine. An 8-bit mixed synchronous controller with self synchronous data path SSRSA architecture is implemented in 40nm CMOS, and operation is measured from 1.3V to 0.4V, with RSA decryption time of 0.16ms, 3x improvement when compared to the fastest state-of-the-art. Side-channel measurements are also performed and after 50,000 measurements employing simple power analysis, differential power analysis (DPA), and high order DPA, no information is leaked by the self synchronous architecture. The design of a self synchronous controller and state machine is then presented, leading to the implementation of a complete self synchronous architecture. We fabricate this architecture twice in 40nm

CMOS with each implementing a different modular exponentiation algorithm, with post-layout simulation results showing an increased operation range down to 0.28V.

Through analysis and results backed up with real chip fabrications and measurements presented in this thesis, we show that dual pipeline self synchronous circuits are a very viable candidate for future variation dominated VLSI, being able to achieve high performance, energy minimum, and error robust operation.