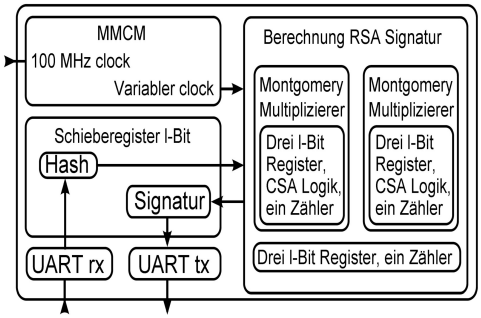
Dorian Amiet

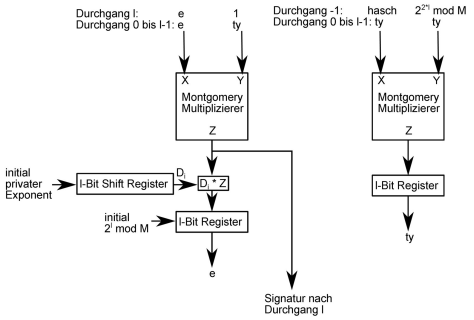
Diplomand	Dorian Amiet
Examinator	Prof. Dr. Paul Zbinden
Experte	Prof. Dr. Paul Zbinden
Themengebiet	Sensor, Actuator and Communication Systems
Projektpartner	Securosys SA, Zürich, ZH

Hardware-Beschleunigung zur Berechnung von digitalen Signaturen

VHDL Implementation schneller RSA Signierung mit variabler Schlüssellänge



Das entwickelte VHDL Design in der Übersicht. Die UART Schnittstelle wird verwendet, um ein Hash zu empfangen und die Signatur zu senden.

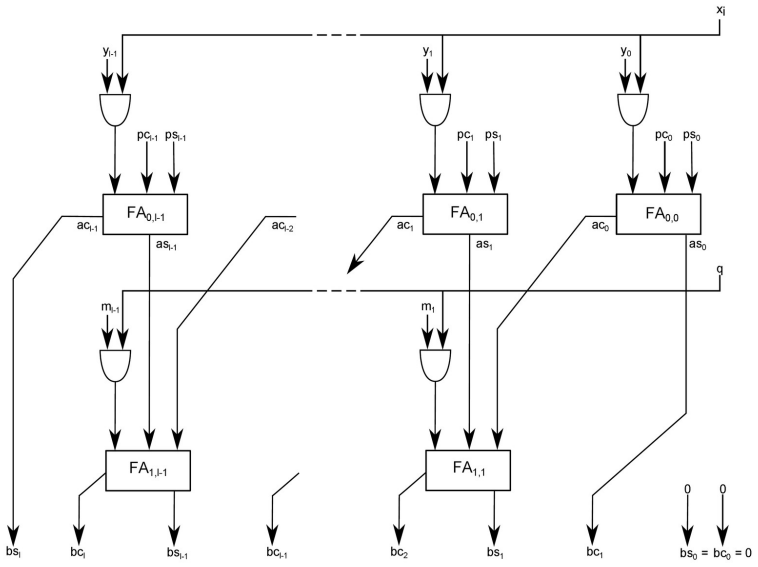


Die RSA Signatur wird mit dem LSB-first Algorithmus berechnet. Dabei kommen zwei Montgomery Multiplizierer zum Einsatz.

Ausgangslage: Die Firma Securosys SA hat sich zum Ziel gesetzt, mit ihren Produkten die Datenübertragung über öffentliche Telekommunikationsnetzwerke zu sichern. Zurzeit wird eine Network-Appliance entwickelt, bei der die Authentisierung mittels digitaler Signatur im Zentrum steht. Dabei gelangen standardisierte kryptografische Verfahren zum Einsatz. Eines der möglichen Verfahren ist die RSA Signierung. Diese baut auf modularen Exponentialfunktionen auf. Aufgrund hoher Anforderungen bezüglich Sicherheit kommen bei RSA Signierungen Schlüssel mit Längen von 3072 Bits und mehr zum Einsatz.

Aufgabenstellung: Aufgrund der langen RSA Schlüssel ist die Berechnung einer Signatur rechenintensiv. Darum sollen die zeitkritischen Algorithmen zur Berechnung der RSA Signatur auf einem FPGA durchgeführt werden. Ein möglichst hoher Datendurchsatz soll hierbei erzielt werden. Die Einhaltung von hohen Sicherheitsstandards sollen Angriffe auf Seitenkanäle erschweren.

Ergebnis: Ein VHDL Design wird entwickelt und im FPGA implementiert. Dieses berechnet die RSA Signatur mit dem LSB-first Algorithmus aus einem gegebenen Hash. Für die Berechnung der modularen Exponentialfunktion wird die Montgomery Multiplikation benutzt. Diese umgeht die Berechnung der Division. Durch den generischen Aufbau des Designs lassen sich die Schlüssellängen variabel einstellen. Die Berechnung einer Signatur mit 512 Bit Schlüssellänge dauert 3.32ms. Dafür werden im FPGA 1160 CLBs benötigt. Für eine 3072 Bit Signatur sind 8830 CLBs und eine Berechnungszeit von 472.92ms nötig.



Die Montgomery Zelle ist das Herzstück des VHDL Design. Diese Logik berechnet die Montgomery Multiplikation. Die CSA Form hält die Pfade kurz.