Hardware-Beschleuniger zur Berechnung der FALCON Signatur

FALCON, einziger NIST-Finalist ohne publizierte Implementierung in Hardware – wirklich nicht hardwaretauglich?

Diplomanden

Andreas Senn

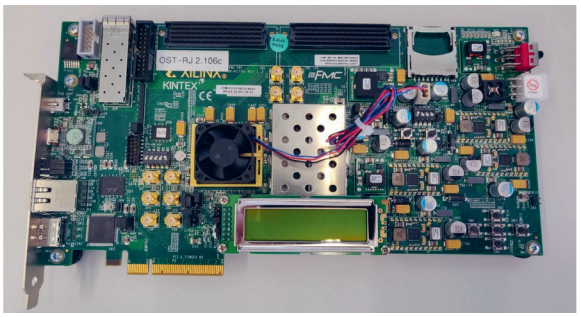
Jan Wendler

Ausgangslage: Die Post-Quantum-Kryptographie erfährt eine immer grösser werdende Bedeutung. Quantencomputer sind theoretisch in der Lage, bestimmte mathematische Funktionen um ein Vielfaches schneller auszuführen als herkömmliche Computer. Sollten Quantencomputer jemals zum Einsatz kommen, bestünde die Gefahr, dass viele digitale Signaturen unsicher werden. Um diesem Problem vorzubeugen, hat das National Institute of Standards and Technology (NIST) einen Wettbewerb ausgeschrieben, um neue Verfahren für digitale Signaturen zu finden, die vor Quantencomputern sicher sind. Nach zwei Runden sind noch drei verschiedene Protokolle im Rennen: Rainbow, CRYSTALS-Dilithium und FALCON. Diese Algorithmen müssen primär sicher sein. Für die Umsetzung in der Praxis, zum Beispiel in den Geräten von unserem Projektpartner Securosys, ist nicht nur die theoretische Sicherheit, sondern auch der Rechenaufwand pro Signatur relevant. Bisher gibt es bereits publizierte Hardwareimplementierungen von Rainbow und CRYSTALS-Dilithium, aber noch keine des FALCON.

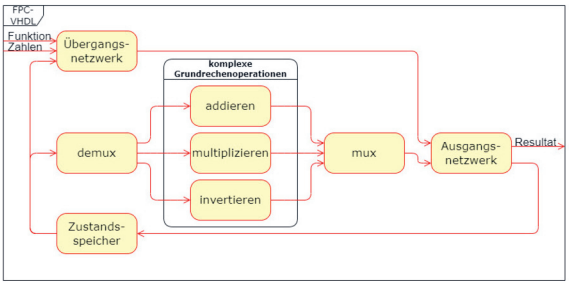
Vorgehen: Um FALCON zu beschleunigen, werden zwei verschiedene Ansätze verfolgt. Der erste Ansatz ist die Beschleunigung einzelner häufig verwendeter Funktionen. Dies ermöglicht es, sehr effiziente Module zu schreiben, die zum Beispiel eine Multiplikation beschleunigen. Das Programm wird auf einem Mikrocontroller ausgeführt, und die beschleunigten Module werden auf einem FPGA implementiert.
Der zweite Ansatz besteht darin, den FALCON-Code mit Vitis HLS nach VHDL zu konvertieren. Mit diesem Ansatz wird das Ziel verfolgt, eine VHDL-Implementation, welche die gesamte FALCON-Signatur berechnet, zu erhalten.

Ergebnis: Im ersten Ansatz wurde mit der Auslagerung der komplexen Rechenoperationen begonnen. Dies verlief problemlos. Durch einige mathematische Umformungen gelang es, ohne Geschwindigkeitseinbussen den benötigten Platz auf dem FPGA zu reduzieren. Alleine durch das Auslagern der komplexen Rechenoperationen konnte die Laufzeit der beschleunigten Funktion um 51% reduziert werden. Eine weitere Funktion wurde auf den FPGA ausgelagert, welche direkten Zugriff auf den Speicher benötigt. Bei der zeitlichen Abstimmung zwischen dem Mikrocontroller und der eigenen Hardware gibt es noch ein Problem, welches auf unklare Optimierungen innerhalb des Mikrocontrollers zurückgeführt werden konnte. Deshalb wurde die Integration dieses Moduls nicht beendet. Dieser Ansatz zeigt, dass ein deutlicher Geschwindigkeitsgewinn mit hardwarebeschleunigten Modulen erzeugt werden kann.
Der zweite Ansatz erwies sich als schwieriger als erwartet. Die Konvertierung von C nach VHDL kann nur unter ganz bestimmten Bedingungen durchgeführt werden. Deshalb mussten einige Funktionen des C-Codes umgeschrieben werden. Nach einiger Arbeit konnte so der C-Code konvertiert werden. Der generierte Block wurde zusammen mit einem Mikrocontroller in einem FPGA implementiert. Dieser zeigt aber noch ein Fehlverhalten auf, welches aus Zeitgründen nicht korrigiert werden konnte. Dadurch ist es leider nicht möglich, den Grad der Beschleunigung genau zu bestimmen. Soweit bekannt, wurde in dieser Arbeit die weltweit erste Hardwareimplementation des Signieralgorithmus designt. Mit etwas mehr Zeit wäre es für beide Ansätze möglich, die verbleibenden Fehler zu beheben.

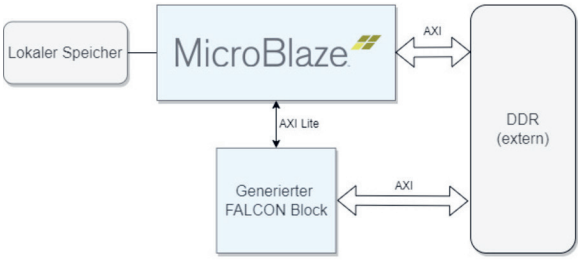
Das in dieser Arbeit verwendete FPGA Board: Kintex KC705
Eigene Darstellung



Übersicht der mit VHDL beschleunigten Rechenoperationen
Eigene Darstellung



Implementation des generierten FALCON-Blocks
Eigene Darstellung



Referent
Prof. Dr. Paul Zbinden, Dorian Amiet

Korreferent
Robert Reutemann, Miromico AG, Zürich, ZH

Themengebiet
Mikroelektronik

Projektpartner
Securosys SA, Zürich, ZH