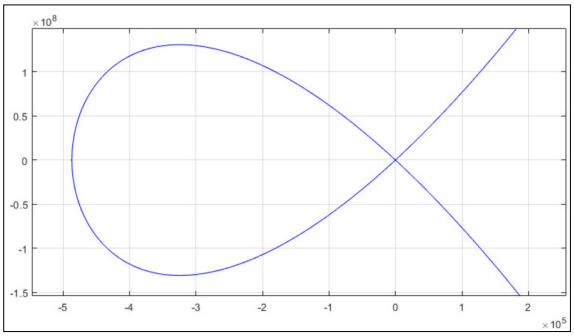
Damian Jurek Wildmann

Diplomand	Damian Jurek Wildmann
Examinatoren	Prof. Dr. Paul Zbinden, Dorian Amiet
Experte	Robert Reutemann, Miromico AG, Zürich, ZH
Themengebiet	Mikroelektronik
Projektpartner	Securosys SA, Zürich, ZH

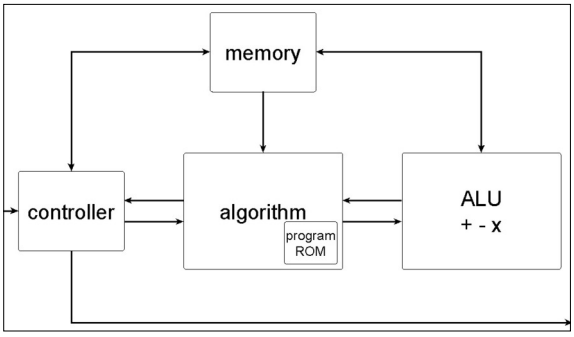
Hardware-Beschleunigung zur Berechnung der Curve25519

VHDL Implementation zur schnelleren Berechnung von Public-Keys und Signaturen

Das Hardware-Sicherheitsmodul von Securosys SA
https://www.securosys.com/



Der Plot der elliptischen Kurve Curve25519
Eigene Darstellung



Die oberste Ebene des Hardware-Beschleunigers: Der controller-Block übernimmt die Kommunikation mit dem Host
Eigene Darstellung

Einleitung: Das Hardware-Sicherheitsmodul (HSM) der Firma Securosys SA ermöglicht es, die Datenübertragung über öffentliche Telekommunikationsnetzwerke zu sichern. Die dafür benötigten Algorithmen, der asymetrische Schlüsseltausch und das Signaturverfahren sind sehr rechenaufwändig. Zur Beschleunigung dieser kryptografischen Verfahren werden im HSM die zeitkritischen Funktionen in einem FPGA implementiert. Für das Verfahren mit der neueren elliptischen Kurve Curve25519 ist dies noch nicht umgesetzt.
Im Rahmen dieser Bachelorarbeit soll ein System entwickelt werden, das die Berechnungen für den asymetrischen Schlüsseltausch und das Signaturverfahren auf der Curve25519 durchführen kann. Dabei soll bei einem möglichst kleinen Ressourcenbedarf ein möglichst hoher Datendurchsatz erreicht werden.

Ergebnis: Es wurde ein Systemdesign entwickelt, das sämtliche Anforderungen erfüllen kann. Das zentrale Element dieses Cores ist die Recheneinheit (ALU). Sie beherrscht die Addition, Subtraktion und Multiplikation von 255-Bit langen Zahlen gefolgt von einer Modulo-Operation. Mittels Instruktionen, welche im Programmspeicher untergebracht sind, wird die ALU angesprochen. Innerhalb des algorithm-Blocks werden die Instruktionen aus dem Speicher gelesen und an die ALU übermittelt. Es sind die Instruktionen für die Punktaddition und Verdoppelung auf der Curve25519 und für die modulare Inversion mit Modulus 2^{255} - 19 hinterlegt.

Das gewählte Design erlaubt eine einfache Erweiterung mit dem Signaturverfahren. Die Operationen können im Programmspeicher abgelegt werden.

Fazit: Das vorliegende System berechnet einen Curve25519 Public-Key in einer Millisekunde. Die FPGA Implementation läuft mit einer Taktfrequenz von 175MHz und benötigt 2403 LUTs, 2859 FFs, 0.5 BRAM und 17 DSP-Slices.
Im Vergleich zu einer öffentlich publizierten FPGA Implementation werden 20% weniger Ressourcen benötigt, die Berechnung dauert dafür doppelt so lange. Im Gegensatz zur publizierten Referenz ist das vorliegende System auf eine Erweiterung zur Berechnung von Signaturen ausgelegt und bietet somit zusätzliche Flexibilität.