

Kurzbericht

ZE: Creonic GmbH	Förderkennzeichen: 16KISQ057
Vorhabenbezeichnung: DE-QOR Design hochperformanter CV-QKD-Module für den flexiblen Einsatz in Quantensicheren Optischen Metro- und Weitverkehrsnetzen Teilvorhaben: Niederratige Fehlerkorrektur für den Schlüsselaustausch in der Quantenkryptographie	
Laufzeit des Vorhabens: 01.01.2022 - 31.03.2025	

Voraussetzungen und Planung der Förderung

Creonic hat Expertise im Bereich mikroelektronischer Schaltungsentwürfe aufgebaut und eine Methodik entwickelt, die komplexe Algorithmen effizient und schnell auf FPGAs implementiert.

Im Ablauf wurden zunächst die Hardwarekomponenten entwickelt und im Anschluss Treiber und Firmware entwickelt, welche funktional getestet wurden. Parallel wurden Algorithmen der Fehlerkorrektur zum Austausch des Schlüsselmaterials umgesetzt.

Ein Demonstrator zur Erprobung der Algorithmik in einem Testaufbau wurden in Betrieb genommen.

Zusammenarbeit

Creonic und das KIT verfolgen einen gemeinsamen iterativen Ansatz für die Entwicklung und Untersuchung geeigneter Fehlerkorrekturverfahren. Das KIT bringt die Expertise des Codesign ein, Creonic das Wissen über die Auswirkungen auf die Hardwareimplementierung. Im Anschluss untersuchte Creonic verschiedene Hardwarearchitekturen mittels Entwurfsraumexploration. Dabei wurden alle relevanten Parameter aufgelistet und deren Auswirkungen auf das Hardwaredesign betrachtet. Zur Verifikation der Ergebnisse wurde eine Architektur auf einer FPGA Hardware implementiert. Diese Plattform wurde zu einem vollständigen FEC Demonstrator weiterentwickelt, der in den Gesamtdemonstrator integriert.

Ergebnisse

Das Projekt hat wichtige Ergebnisse in zwei Bereichen erzielt: der Entwicklung sicheren Übertragungssystemen zum Schlüsselaustausch und der Erprobung neuer Hardwareplattformen. Im Bereich der ML-basierten Übertragungssysteme wurde ein Demonstrator entwickelt, der

Rahmen dieses Projekts wurde die hardwarenahe Umsetzung der zuvor entwickelten Softwaremodelle auf einer FPGA-Plattform erfolgreich realisiert. Dabei wurden ein LDPC-Encoder für die Senderseite sowie ein speicheroptimierter Decoder für niedrige Coderaten auf der Empfängerseite implementiert. Die funktionale Korrektheit der entwickelten IP-Cores wurde durch umfangreiche Co-Simulationen mit den Softwaremodellen verifiziert. Parallel dazu entstand ein eigenständiger Demonstrator zur Echtzeitprüfung, der die Komponenten für Fehlerkorrektur (FEC) und Reverse Reconciliation (RR) vereinte. Für die RR-Logik wurden mehrere optimierte Implementierungsgenerationen entwickelt, die erfolgreich auf einem FPGA getestet wurden.

Bei der Fehlerkorrektur erwiesen sich LDPC-Codes gegenüber Polar oder Turbocodes als besser geeignet. Es wurden konkrete Codeparameter festgelegt, darunter eine minimale Coderate von 1/100 und eine Blockgröße von 100.000 Bits. Bitgenaue Softwaremodelle von Encoder und Decoder wurden entwickelt und optimiert, unter anderem durch Layered Decoding und Early Termination, was die Dekodierlatenz halbierte und den Durchsatz erhöhte. Die Modelle wurden in Langzeitsimulationen unter realistischen Kanalbedingungen getestet, wobei die funktionale Korrektheit und die Bitfehlerrate (BER) bestätigt wurden.

Zwei verschiedene Decoder-Architekturen wurden in Hardware umgesetzt. Während Variante 1 zu ressourcenintensiv für die Zielplattform war, erwies sich Variante 2 als geeigneter: Sie bot trotz geringerer Komplexität eine höhere interne Auflösung und mehr Iterationen, was sich positiv auf die Kommunikationsleistung auswirkte. Daher wurde Variante 2 für die finale Systemintegration ausgewählt.

Zur Unterstützung der Zusammenarbeit im Konsortium wurde eine erste Datenschnittstelle auf Basis von gRPC implementiert, die trotz begrenztem Durchsatz eine effektive parallele Entwicklung ermöglichte. Abschließend wurde der finale Gesamtdemonstrator gemeinsam mit den Projektpartnern aufgebaut. Die Integration aller Komponenten – Encoder, Decoder und RR-Logik – verlief erfolgreich, und das System konnte in mehreren Testkampagnen unter Echtzeitbedingungen überzeugen. Besonders hervorzuheben ist die zuverlässige Fehlerkorrektur selbst bei extrem niedrigen Signal-Rausch-Verhältnissen bis -20 dB.

Insgesamt wurden alle Ziele des Projekts erreicht: Die IP-Cores wurden implementiert, verifiziert und in ein funktionierendes Gesamtsystem integriert. Die Wahl der ressourcenschonenderen Decoder-Variante war dabei ein entscheidender Erfolgsfaktor.