



# Quantenkryptographie in speziell gekapselter Hardware

www.quantenkryptographie.at

M. Meyenburg, T. Lorüner, O. Maurhart, M. Peev, M. Suda, F. Schupfer, E. Querasser

ARC Seibersdorf research GmbH, Donau-City-Strasse 1 / 4.0G, A-1220 Wien

## Motivation

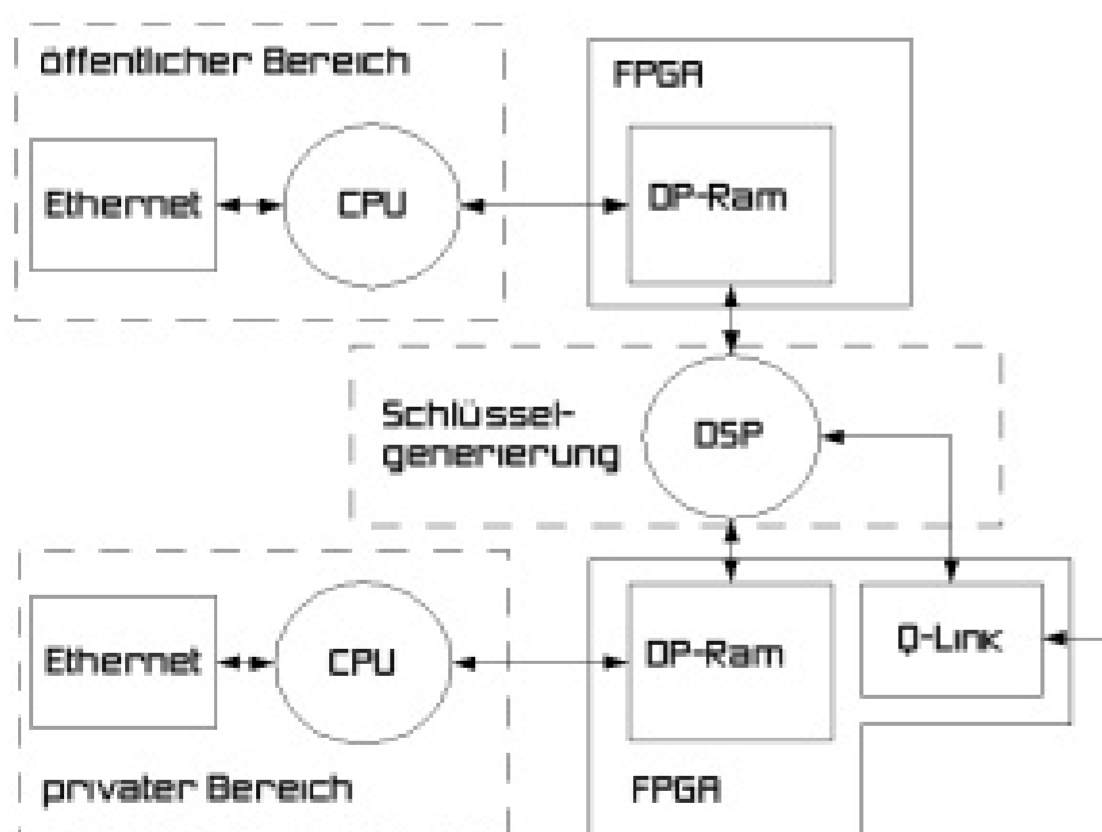
Die Absicherung von Computer-Netzwerken gewinnt immer mehr an Bedeutung und so haben sich viele Lösungen am Markt platziert deren Sicherheitsniveau fragwürdig oder deren praktikabler Einsatz ungünstig sind. Der Einsatz von Quantenkryptographie mit einer speziell für diesen Bereich abgestimmten embedded Hardwarelösung ermöglicht einen sehr hohen Sicherheitslevel trotz einfachem Betrieb und minimaler Konfiguration. Durch Integration und Zusammenfassung in einem Chip ist eine weitere Steigerung der Datenraten möglich.

Quantenkryptographie erlaubt die Generierung von identischen kryptographischen Schlüsseln an zwei verschiedenen Orten, wobei Dritten das Abhören aufgrund quantenphysikalischer Gesetze unmöglich gemacht wird. Der hohe Sicherheitsstandard von Quantenkryptographie versteht sich von selbst doch ebenso muss die Hardware diesen extremen Kriterien entsprechen, denn die Kette verwendeter Komponenten ist nur so stark wie das schwächste Glied. So muss bei der Entwicklung der Elektronik, Entwurf der Software und Kombination der Elemente massiven Wert auf Sicherheit gelegt werden.

Einerseits wird dem Gerät die schnelle und hochgenaue Detektierung von Quantenkorrelationen andererseits die räumlich Trennung der Schlüsselgenerierung und Kommunikation abverlangt. Diese Trennung ist ein wesentlicher Punkt im Sicherheitskonzept, um die Möglichkeit von Codeeinschleusung und den damit verbundenen Zugriff auf den generierten Schlüssel zu vermeiden. Weiters benötigt die Ermittlung der Korrelationen ein hochgenaues und zeitkritisches System, welches flexibel und schnell auf störende Umwelteinflüsse reagieren und automatisch nachjustieren soll.

## Hardwaredesign

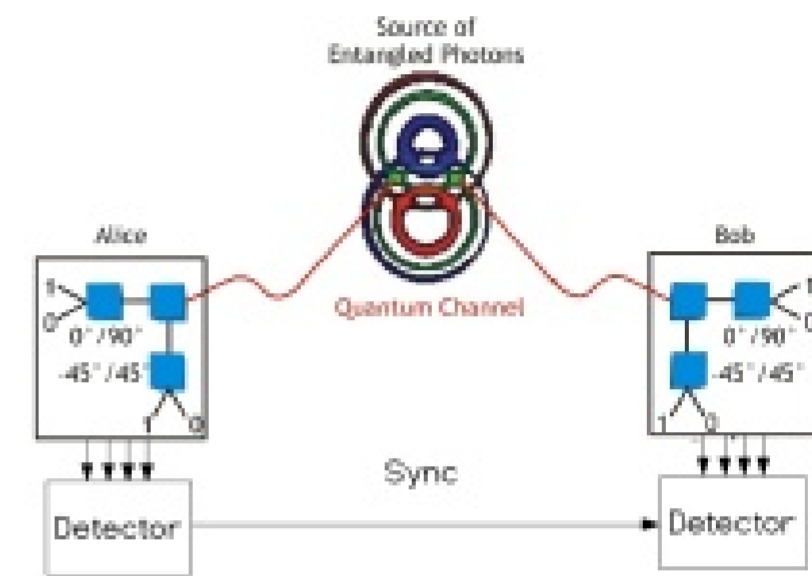
Durch die Trennung der sicherheitskritischen Bereiche und der klassischen Kommunikationseinrichtungen wurde eine Kapselung des erzeugten Schlüssels und der Verschlüsselung selbst geschaffen. Diese Abgränzung gewährleistet ein hohes Maß an Sicherheit. Somit können Standardkomponenten gewählt werden, die hohe Flexibilität bei niedrigem Entwicklungsaufwand garantieren.



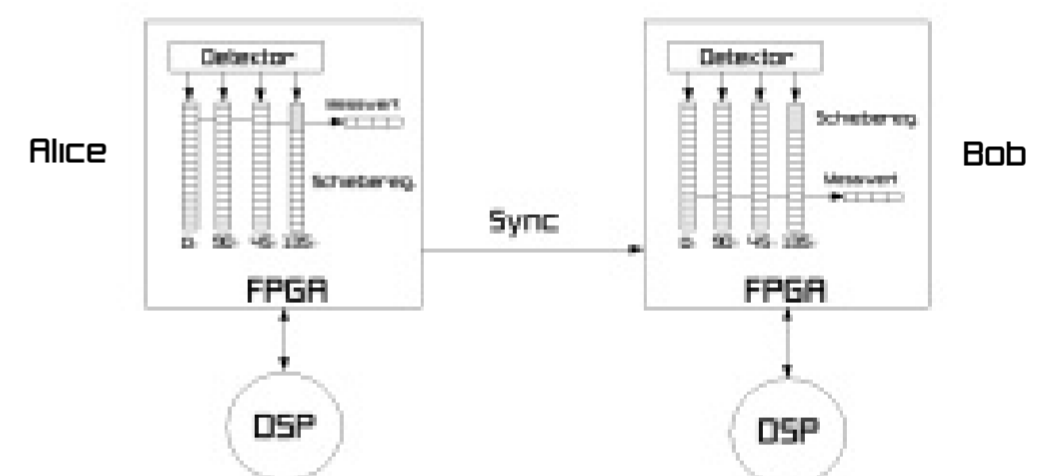
Sollte durch eine externe aber auch interne Attacke die jeweiligen Betriebssysteme der CPU's beeinflusst werden, so ist immer noch kein Zugriff auf die Schlüsseldaten möglich, die nur in der gekapselten Umgebung des DSP-Bereiches verfügbar sind.

## Messmethodik

Der Schlüsselaustausch<sup>1</sup> wird mittels Verschränkung von Photonen und Messung in zwei verschiedenen Basen realisiert. Eine Seite generiert nach Detektion eines Photons einen Syncimpuls der die Gegenstelle veranlasst, auch eine Messung durchzuführen.

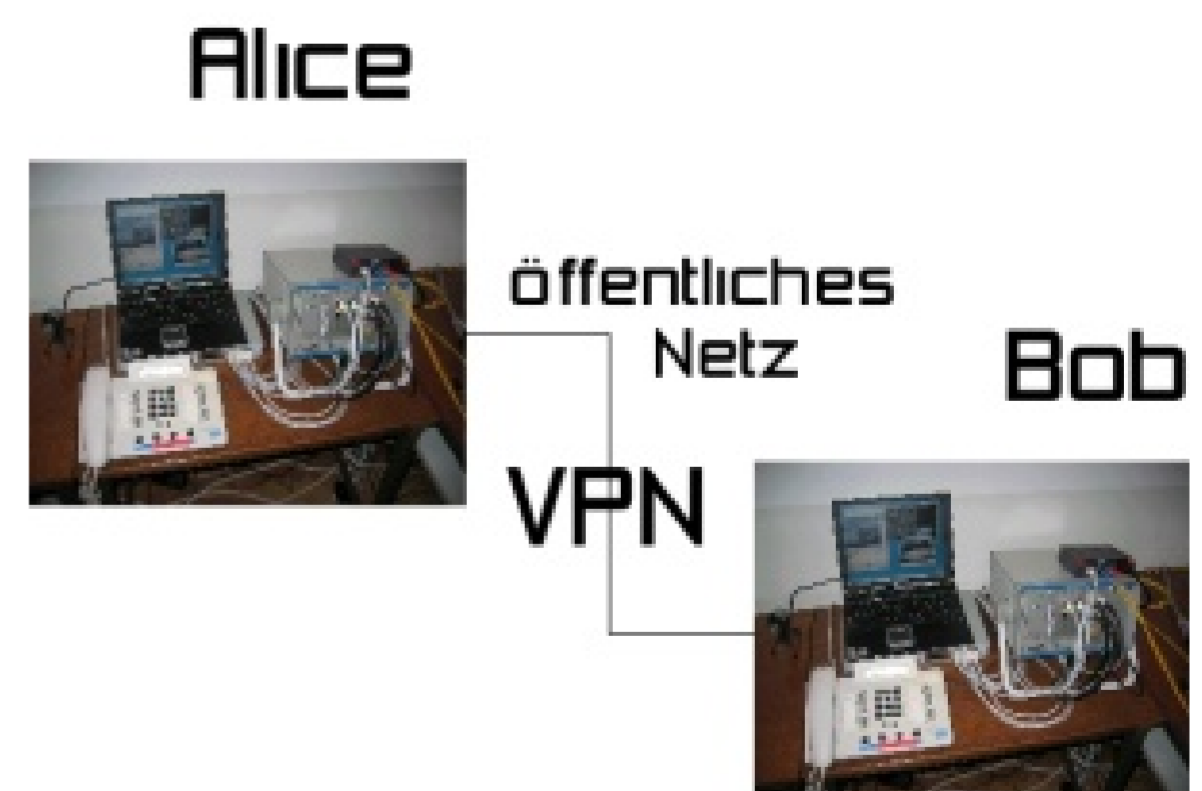


Die zeitliche Differenz von Sync und Messwerten muss präzise ausgeglichen werden und in einer Auflösung im Bereich von Nanosekunden geschehen. Solch hohe Genauigkeiten können nur unter erheblichem Aufwand realisiert werden, da die Verschiebung nicht nur exakt sondern auch frei einstellbar sein muss. Realisiert wurde diese Anforderung mittels vier extrem schnellen Schieberegistern, die die Detektorsignale seriell verarbeiten und bei einem Sync einfrieren.



## Anwendung

Die erzeugten Schlüssel können für eine One-Time-Pad- aber auch für AES-Verschlüsselung verwendet werden, wobei AES höhere Datenraten erlaubt aber die absolute Sicherheit theoretisch nicht beweisbar ist. Ein mögliches Szenario ist eine VPN-Verbindung zweier Netze.



## Referenzen

[1] ... R. Poppe et al., "Practical Quantum Key Distribution with Polarisation Entangled Photons", arXiv:quant-ph/0404115v2, 2004