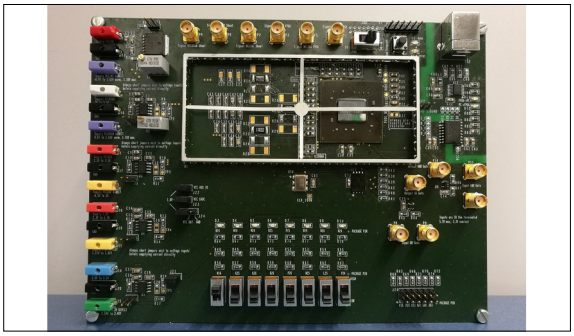
Alex
Weber

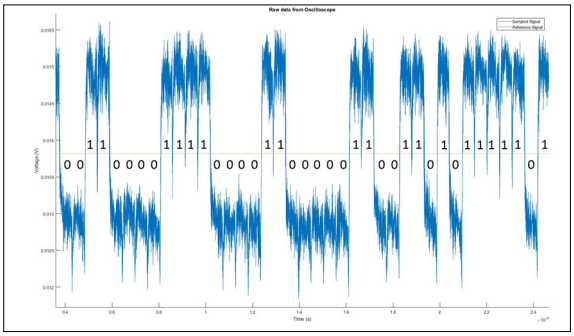
Patrick
Willi

Studenten	Alex Weber, Patrick Willi
Examinatoren	Prof. Dr. Paul Zbinden, Lukas Leuenberger
Themengebiet	Mikroelektronik
Projektpartner	Securosys SA, Zürich, ZH

FPGA Plattform zur Messung von Seitenkanälen



Das fertige Board



Auswertung der Messdaten: Die Bits des Schlüssels

Einleitung: Die Kryptographie wird immer wichtiger in der modernen digitalen Welt. Insbesondere Transaktionen im Finanzmarkt müssen besonders gut vor Manipulation und Einsicht unberechtigter Personen geschützt werden. Die dazu verwendeten Algorithmen gelten als sehr sicher und die Länge der Schlüssel garantieren, dass es zu lange dauern würde, alle möglichen Kombinationen durchzuprobieren. Die langen Schlüssel führen aber auch dazu, dass die Berechnungen auf einem Prozessor zu langsam wären, um den heutigen Anforderungen gerecht zu werden. Deshalb werden sie auf eigens dafür gemachte Hardware ausgelagert. Die Firma Securosys SA ist ein Hersteller solcher Hardware, welche FPGAs für die Beschleunigung der Algorithmen verwendet. Jedoch nützt auch eine sichere Verschlüsselung nichts, wenn die Implementation nicht geschützt ist: Wenn man den Algorithmus nicht knacken kann, sucht ein potenzieller Angreifer seine Chancen in den sogenannten Seitenkanälen. Dies sind unbeabsichtigte Informationslecks, die von der Implementation her stammen und nicht ein inhärenter Teil des Algorithmus sind. So variiert zum Beispiel der Stromverbrauch in Abhängigkeit davon, was auf dem Chip gerade gerechnet wird und es werden unterschiedliche elektrische Felder abgestrahlt. Diese Seitenkanäle können nicht verhindert werden. Deshalb muss sichergestellt werden, dass aus ihnen keine brauchbaren Informationen gewonnen werden können.

Aufgabenstellung: Ob es den Entwicklern gelungen ist, die Menge an brauchbaren Informationen in den Seitenkanälen zu reduzieren, muss mittels Messungen ermittelt werden. Das Ziel dieser Arbeit war es, eine dazu geeignete Messeinrichtung zu entwickeln. Wichtige Kriterien dabei waren, die Stromversorgung möglichst frei von störendem Rauschen zu halten und möglichst einfache und gute Messungen zu ermöglichen. Dazu wird der Strom mittels Spannungsabfall über einem Shunt gemessen. Um auch Messungen der elektromagnetischen Felder zu ermöglichen, sollte der Chip gut erreichbar, aber gleichzeitig auch vor Strahlung von aussen geschützt sein. Das Board soll eine Schnittstelle zum Computer, ein Interface zum Debuggen, einen Speicher zum automatischen Beschreiben des FPGA und einige Bedienelemente haben. Der Typ des FPGAs wurde vorgegeben, es soll ein XC7K160T mit 676 Pads eingesetzt werden.

Ergebnis: Es wurden ein Schaltplan und ein daraus resultierendes Layout für ein PCB erstellt. Anschliessend wurde das PCB hergestellt, bestückt und erfolgreich in Betrieb genommen. Bei der Inbetriebnahme sind kleine Fehler im Design festgestellt worden. Diese wurden im Schema wie auch im Layout korrigiert. Vom HSR Institut IMES wurde uns eine Implementation des RSA-Algorithmus zur Verfügung gestellt, um eine Seitenkanalattacke durchzuführen. Mit einem Oszilloskop wurde der Stromverlauf aufgezeichnet und im Matlab analysiert. Die durchgeführten Messungen waren sehr zufriedenstellend bezüglich Signalhub und Rauschen. Die Messresultate zeigten, wie einfach es ist, den Schlüssel herauszufinden, wenn die Implementation nicht gegen einen solchen Angriff geschützt ist.