Kurzfassung

Hochleistungsrechner aus rekonfigurierbarer Hardware für Anwendungen in der Kryptoanalyse

Heutzutage haben wir uns angewöhnt, zu jedem Zeitpunkt unsere Gedanken, Gewohnheiten und Bekanntschaften in sozialen Netzwerken zu teilen. Hierzu nutzen wir netzwerkbasierte Dienste wie das intelligente Stromnetz, ferngesteuerte Haustechnik oder das Internet der Dinge. Im gleichen Maße, in dem die Verbindung zwischen Mensch und Netzwerk sowie der Datenfluss ansteigen, wächst die Bedeutung eines verlässlichen Schutzes vor Datenmissbrauch. Dazu vertrauen wir auf kryptographische Primitive, die wir zum Schutz von Datenintegrität, -authentizität und -vertrauenswürdigkeit einsetzen. Diese Primitive müssen dabei so lange als sicher gelten, wie die Daten potenziell Verwendung finden können. Die Geschichte hat gezeigt, dass Kryptoanalyse nicht nur eine theoretische Bedeutung hat, sondern auch unter Berücksichtigung des aktuellen Standes der Technik erfolgen muss. Durch die Verwendung optimaler Angriffe in Kombination mit der modernsten Hardware lässt sich das Sicherheitslevel kryptographischer Algorithmen nach oben abschätzen. Dadurch können frühzeitig Anpassungen an die Sicherheitsparameter oder der Austausch von Algorithmen vorgeschlagen werden.

Der Fokus dieser Arbeit liegt in der Analyse der Einflüsse der Verwendung von Hardwarebeschleunigung durch Hochleistungsrechner aus rekonfigurierbarer Hardware für die Anwendungen in der Kryptoanalyse. Zudem werden die daraus resultierenden Auswirkung auf die Sicherheitsabschätzungen untersucht. Da nicht alle kryptographischen Primitive gleichermaßen für eine Hardwareimplementierung geeignet sind, werden in dieser Arbeit vier Projekte aus verschiedenen Teilgebieten der Kryptologie, insbesondere aus dem Bereich der Stromchiffren, effizienter Passwortsuche, Elliptische-Kurven-Kryptographie und Post-Quantum Kryptographie dargestellt:

Im ersten Projekt wird ein neuer algebraischer Angriff, der auf einer verbesserten Version der Cube Tester basiert, gegen die Stromchiffre Grain-128 beschrieben. Die Validierung des Angriffs unter Verwendung eines Simulationsalgorithmuses erfordert darauf spezialisierte Hardware, da ein Software-Ansatz nicht effizient genug ist. Das zweite Projekt beschäftigt sich mit der effizienten Passwortsuche gegen Schlüsselableitungsfunktionen und untersucht die Sicherheit zwei der derzeitigen Standards in der Passwortableitung: PBKDF2 und bcrypt. Dabei werden die Auswirkungen von spezialisierter Hardware für energieeffiziente Angriffe und Kontrahenten mit entsprechenden finanziellen Mitteln analysiert. In dem dritten Projekt geht es um die Berechnung des diskreten Logarithmus Problems auf der elliptischen Kurve sect113r2, die eine bislang nicht gebrochene Binärkurve der SECG Standardkurven über dem $\mathbb{F}_{2^{113}}$ ist. Dabei wurde der parallele Pollard's Rho Algorithmus zum ersten Mal in Hardware in Kombination mit der Negation Map Technik implementiert, um die Effizienz der Random Walk Iteration zu erhöhen. Der letzte Abschnitt handelt von der ersten hardwarebeschleunigten Implementierung eines Information Set Decoding Angriffs auf das Post-Quantum Kryptographieverfahren McEliece. Die Proof-of-Concept Implementierung dient dabei als Grundlage für die Diskussion der Vorteile

und Einschränkungen durch den Hardware-Entwurf, die signifikante Unterschiede in der Wahl der Parameter und Optimierungen nach sich ziehen.

Die Resultate der Projekte zeigen, dass in den verschiedenen Bereichen der Kryptoanalyse der Einsatz von Hardwarebeschleunigung unterschiedliche große Auswirkungen mit sich bringt. Dennoch rücken Hochleistungsrechner und hochparallele Implementierungen immer stärker in den Fokus der Sicherheitsforscher, da die Kosten für die Durchführung von Angriffen immer attraktiver werden. Dementsprechend wird inzwischen bei der Definition neuer kryptographischer Primitive viel Wert auf Maßnahmen gegen Vorteile eines Angreifers durch massive Parallelisierung und energie-effiziente Implementierungen gelegt.

Schlagworte

Kryptoanalyse, Rekonfigurierbare Hardware, FPGA, Hochleistungsrechner, Hochgeschwindigkeitsberechnungen, Implementierung.