Diese Arbeit analysiert den Einfluss von Hochleistungsrechnern aus rekonfigurierbarer Hardware in der Kryptoanalyse und die Auswirkungen auf die Sicherheitsabschätzungen. Da nicht alle kryptographischen Primitive gleichermaßen für eine Hardwareimplementierung geeignet sind, werden vier Projekte aus verschiedenen Teilgebieten der Kryptologie, insbesondere Stromchiffren, effiziente Passwortsuche, Elliptischen Kurven und Post-Quantum Kryptographie, dargestellt.

Die Resultate zeigen, dass in verschiedenen Bereichen der Kryptoanalyse der Einsatz von Hardwarebeschleunigung unterschiedlich große Auswirkungen hat. Dennoch rücken Hochleistungsrechner und hochparallele Implementierungen immer stärker in den Fokus, da die relativen Kosten für die Durchführung von Angriffen immer attraktiver werden. Bei der Definition neuer kryptographischer Primitive wird daher viel Wert auf Maßnahmen gegen die Ausnutzung massiver Parallelisierung und energieeffizienter Implementierungen eines Angreifers gelegt.