# Anwendung Quadratischer Funktionen zur Sicherung des Hashwertes

Die ASH-20 Hashfunktion setzt nicht nur auf grundlegende mathematische Operatoren, sondern integriert auch geschickt quadratische Funktionen, um die Sicherheit und Einweg-Natur des Hashwertes zu verstärken. Die Verwendung solcher Funktionen höheren Grades bringt eine zusätzliche Komplexität in die Hashberechnung, die es potenziellen Angreifern erheblich erschwert, den Ursprung des Hashwertes zurückzuverfolgen.

## Funktionsweise quadratischer Funktionen

Als Beispiel dient eine quadratische Funktion $f(x) = ax^2 + bx + c$, wobei $a$, $b$, und $c$ Parameter sind, die durch die Hashfunktion bestimmt werden. Die Anwendung dieser Funktion auf Teile des Hashwertes sorgt für nichtlineare Verzerrungen, die selbst bei minimalen Eingangsänderungen dramatische Auswirkungen auf den resultierenden Hash haben.

## Rechenbeispiel

Nehmen wir an, der ursprüngliche Hashwert sei $H$, und die quadratische Funktion $f(x)$ werde auf einen Teil des Hashwertes angewendet: $f(H) = aH^2 + bH + c$. Selbst bei einer geringfügigen Veränderung von $H$ führt dies zu einem neuen, scheinbar zufälligen Wert. Zum Beispiel:

Wenn $H = 123$, dann $f(123) = 5 \times 123^2 + 2 \times 123 + 7 = 76258$.

Bei einer minimalen Änderung, $H' = 124$, ergibt sich jedoch $f(124) = 5 \times 124^2 + 2 \times 124 + 7 = 78731$.

Diese nichtlineare Reaktion auf Eingangsänderungen, kombiniert mit anderen Hash-Operationen, schafft eine robuste Barriere gegen Rückverfolgungsversuche. Die ASH-20 Hashfunktion beweist so ihre Effektivität in der Sicherung von Datenintegrität in kryptografischen Anwendungen.