Projekt: Kryptografie mit elliptischen Kurven

Leon Groß 108018221971
Auswertung Benchmarking

June 18, 2019

Die Werte der folgenden Tabelle enstammen einem Benchmarking mit n = 10^4

	extended_euclidian_algorithm	fermats_little_theorem
Non-adjacent Form	$\approx$ 48 min	$\approx$ 108 min
Double-And-Add	$\approx$ 72 min	$\approx$ 156 min

Es stellt sich heraus, dass die *NAF* durch ihre durchschnittlich signifikant geringere *Hamming-Weight* c.a. $\frac{2}{3}$ der Rechenzeit im Vergleich zu der Verwendung des DA benoetigt; die NAF ist dem DA in der Performance weit ueberlegen.

Vergleicht mab nun noch die Laufzeit des erweiterten euklidschen Algorithmus' mit der des kleinen Fermat'schen Theorem erkennt man, dass der EEA mit etwa halber Laufzeit des Fermat eine deutlich bessere Performance aufweist. Dies ist auf die rechenintensiven Potentierungen mit dem Sqaure and Multiply Algorithmus, auf welchem Fermat basiert, zurueckzufuehren.

Es ist final festzuhalten, dass die Komibantion der beiden performantesten Vorgehensweisen (EEA und NAF) zu dem besten Ergebnis mit c.a. 50 min Laufzeit fuehren.

Das Format der zu entschluesselnden Datei ist PNG.