Randomisatie

Het maken van een kopie van een polymorfe vorm (Polymorfe identiteit/pseudoniem, Versleutelde Identiteit/Pseudoniem) dat cryptografisch niet te herleiden is naar het origineel.

Een polymorfe vorm is technisch gezien een ElGamal versleuteld bericht en met randomisatie maakt men een nieuw versleuteld bericht met dezelfde inhoud, maar dat er 'aan de buitenkant' anders uitziet. Voor randomisatie is geen geheime sleutel benodigd.

Omdat randomisaties ook buiten de HSM kunnen worden uitgevoerd, wordt dit in detail gespecificeerd. Een PI, PP, VI en VP bestaan elk uit drie punten op een elliptische curve, (P, Q, S). Bij randomisatie wordt een willekeurig (‘random’) getal r gekozen met 0 < r < q waar q de grootte van de elliptische groep is. De gerandomiseerde vorm is (P + r*S, Q + r*S, S).