Het trapdoor principe

Een groot deel van de efficiëntie van een cryptografisch systeem berust op de eenvoud waarmee informatie versleuteld en ontsleuteld kan worden wanneer de benodigde parameters bekend zijn, en de moeilijkheid van de ontsleuteling wanneer deze deels of niet bekend zijn. Het doel van het versleutelen van informatie is immers het afschermen van de informatie voor partijen die niet specifiek toegang tot de informatie verleend zijn. Dit mag echter geen hinder vormen voor de vertrouwde partijen. Een cryptografisch systeem moet zodoende beschikken over de eigenschap dat zij eenvoudig toepasbaar is, maar lastig omkeerbaar door kwaadwillenden. Een functie die deze eigenschappen bezit wordt een trapdoor-functie genoemd Dit is een metafoor voor een werkelijk valluik: één richting volgen moet eenvoudig zijn, de tegengestelde richting niet. De trapdoor-functie in dit verslag zal het Diffie-Hellman protocol zijn, welke zich baseert op de theorie van elliptische krommen over eindige velden van priem orde. Het achterliggend probleem dat de veiligheid van dit protocol waarborgt is het elliptische kromme discreet logaritmisch probleem.