



## ‘Ik wil de digitale wereld beveiligen’

**Prof.dr. Tanja Lange (35)**

Hoogleraar cryptologie sinds 2006

Technische Universiteit Eindhoven

‘Het komt inderdaad voor dat cryptologie en versleuteling worden geassocieerd met spionage. Dat stigma kleeft eraan, waarschijnlijk omdat veel mensen onmiddellijk denken aan het kraken van de Enigma-code in de Tweede Wereldoorlog. Of ze denken aan het hacken van computersystemen. Maar heus, ik sta aan de goede kant!

‘Wij cryptologen zijn juist druk bezig om de digitale wereld zoveel mogelijk te beveiligen,

zodat je bankrekening niet wordt geplunderd en je mobiele-telefoongesprekken niet worden afgeluisterd.

‘Waarmee ik natuurlijk niet wil zeggen dat wat ik doe niet spannend is. Integendeel, het is een enorme uitdaging om grote systemen zo te versleutelen dat ze niet open te breken zijn.

‘Wij evalueren de veiligheid van RSA en ECC, de twee meest gebruikte systemen voor cryptografie met publieke sleutels. Samen met de Amerikaanse hoogleraar Daniel J. Bernstein leid ik op dit ogenblik een internationale groep van 23 onderzoekers om met behulp van

nieuwe ideeën en de rekenkracht van enkele clusters een grote uitdaging aan te vallen.

‘Cryptologie is een zeer internationaal vakgebied en de Technische Universiteit Eindhoven speelt er een sterke rol; daarom was het voor mij ook aantrekkelijk om er hoogleraar te worden.

‘In 2008 heb ik samen met dezelfde Bernstein en mijn promovenda Christiane Peters het wereldnieuws gehaald door de McEliece-encryptie te kraken. Het McEliece-systeem bestaat al sinds de jaren zeventig en is nog steeds een goede kandidaat voor het beveiligen van het toekomstige internet, maar dan wel met grotere sleutels. Er moeten veiligere en efficiëntere versies komen, en daar zijn we nu volop mee bezig.’