datanews

Belgische thesis maakt werk van 'kwantumbestendige' cryptografie

12/12/18 om 11:37 - Bijgewerkt om 11:51 Bron: Datanews

BELCLIV, de Belgische Club voor Informaticaveiligheid, heeft de thesis van KU Leuven-student Ward Beullens gelauwerd als beste masterthesis die een bijdrage levert tot de beveiliging van informatiesystemen. Zijn werk is in de running om een post-kwantum-standaard te worden.

© iStock

De jury van BELCLIV beloonde de masterthesis getiteld '*New Signature Schemes based on UOV with smaller public keys*' van Ward Beullens met een geldprijs van 2.000 euro. Beullens schreef de thesis in het kader van zijn Master in Wiskunde aan de KU Leuven, onder leiding van professor en cyptografie-expert Bart Preneel. De Belgische Club voor Informaticaveiligheid (http://www.clusib.be/wp/?lang=nl) rijkt de prijs al voor de vierde keer uit.

Wat als de kwantumcomputer er is?

Zijn thesis draait rond de overschakeling naar nieuwe cryptografie die resistent is tegen mogelijke aanvallen van kwantumcomputers. Zo'n kwantumcomputer zou in theorie gebruikt kunnen worden om alle publieke-sleutel-cryptografie die vandaag in gebruik is, te breken. Heel wat organisaties zoals
Google (/ict/nieuws/google-en-volkswagen-gaan-samen-kwantumcomputeren/article-normal-923709.html)
, Intel,
IBM (/ict/nieuws/ibm-vindt-bewijs-dat-kwantumcomputers-sneller-zijn/article-normal-1382393.html)
maar ook de NSA investeerden al honderden miljoenen in onderzoek naar kwantumcomputers en proberen er
een te bouwen (/ict/nieuws/ibm-bouwt-kwantumcomputer-voor-wetenschap-en-bedrijfsleven/article-normal-823649.html)
. Zo'n kwantumcomputer laat exponentiële rekenkracht toe en die zou ook de bestaande cryptografie kunnen breken. Dat betekent geheime communicatie ontcijferen, maar evengoed ook geïnfecteerde updates pushen naar computers en smartphones om zo de controle van iemand zijn toestel over te nemen.

Nieuwe cryptografie

"Om dit te vermijden moeten we tijdig overschakelen naar nieuwe cryptografie die resistent is tegen aanvallen van kwantumcomputers, zogenaamde Post-Kwantum cryptografie. Mijn thesis gaat over het verbeteren van zo'n Post-Kwantum algoritme", aldus Ward Beullens.

Concreet ontwikkelde hij twee methodes om de grootte van de publieke sleutel veel kleiner (tot wel 15 keer) te maken. Dat maakt dit soort algoritmes veel aantrekkelijker, want de grootte van de sleutel was tot nu toe het grootste nadeel van het algoritme.

Basis voor nieuwe standaard?

Mogelijk komt er zelfs nog een vervolgluik voor Ward Beullens. Zijn werk is ondertussen ook ingezonden naar het Amerikaanse National Institute of Standards and Technology (NIST) dat momenteel een wedstrijd heeft rond goede post-kwantum cryptografie algoritmes. Als Ward Beullens de wedstrijd wint wordt zijn werk mogelijk een post-kwantum standaard.

Dat zou overigens niet eens een primeur zijn voor België. Eerder organiseerde NIST een gelijkaardige wedstrijd om AES te standaardiseren: de Advanced Encryption Standard zoals die wereldwijd momenteel gebruikt wordt.
Die wedstrijd werd gewonnen (/ict/nieuws/aes-10-jaar-belgisch-succes/article-normal-325577.html)
door het Belgische 'Rijndael': een cryptografisch algoritme bedacht door Joan Daemen en Vincent Rijmen. De naam Rijndael is een afgeleide van hun achternamen.

Lees ook:
AES: 10 jaar Belgisch succes (/ict/nieuws/aes-10-jaar-belgisch-succes/article-normal-325577.html)