Kryptografia ja CRYSTALS Kyber

Eemeli Lottonen
eemeli.lottonen@insta.fi

Tutkielmassa tarkastellaan CRYSTALS Kyber -avainten kapselointimekanismia. Yhdysvaltalainen National Institute of Standards and Technology (NIST) on järjestänyt Post Quantum Cryptography -hankkeen (PQC-hanke), jossa pyritään löytämään kvanttilaskentaa kestäviä salausmenetelmiä. Hanke julkaistiin konferenssissa PQCrypto vuonna 2016 ja siihen on lähetetty monia algoritmiehdokkaita, joista yksi on CRYSTALS Kyber. Hanke edistyy kierroksittain ja jokaisella kierroksella huonoimpia ehdokkaita karsitaan pois. CRYSTALS Kyber on päässyt hankkeen kolmannelle kierrokselle.

Tutkielmassa tutustutaan ensin todennäköisyyslaskentaan ja erityisesti satunnaismuuttujiin sekä keskitettyyn binomijakaumaan. Tämän jälkeen esitellään algebraa ja tekijärenkaat. Sitten siirrytään kryptografian peruskäsitteisiin symmetriseen ja epäsymmetriseen salaukseen, hajautusfunktioihin sekä avaintenkapselointiin. Perusasioiden esittelyn jälkeen tutkitaan häirityn oppimisen ongelmaa ja sen eri muotoja. Kyberin turvallisuus perustuu häirityn oppimisen ongelman moduliversioon.

Ongelma esitellään, mutta turvallisuustodistuksia ei. Tämän jälkeen tarkastellaan itse Kyberiä. Se koostuu epäsymmetrisestä salausskeemasta sekä avainten kapselointiosasta. Epäsymmetrinen salausskeema esitellään ensin, jonka päälle rakennetaan avainten kapselointiskeema. Molemmat sisältävät kolme algoritmia, avainten generoinnin, viestin salauksen sekä viestin avaamisen. Tarkastellaan näitä algoritmeja ja todistetaan niiden oikeellisuus. Tarkastellaan sitten Kyberin parametrivalintoja ja vertaillaan kuinka ja miksi ne ovat muuttuneet ensimmäisestä esityskerrasta vuonna 2017. Lopuksi suoritetaan Kyberin suorituskykymittaus käyttäen kolmannen kierroksen ehdokkaan referenssitoteutusta apuna.

Algoritmi 6.4 Kyber.KeyGen: Avainten generointi

1: $\rho, \sigma \leftarrow \{0,1\}^{256}$
2: $\mathbf{A} \sim R_q^{k \times k} := \mathrm{XOF}(\rho)$
3: $(\mathbf{s}, \mathbf{e}) \sim \mathbb{B}_\eta^k \times \mathbb{B}_\eta^k \rightsquigarrow \mathrm{XOF}(\sigma)$
4: $\mathbf{t} = \mathrm{Compress}_q(\mathbf{As} + \mathbf{e}, d_t)$
5: $z \leftarrow \{0,1\}^{256}$
6: **return** $(\mathrm{pk} = (\mathbf{t}, \rho), \mathrm{sk} = (\mathbf{s}, z, \mathbf{t}, \rho))$

KYBERISTÄ YLEISESTI

CRYSTALS Kyber on avainten kapselointimekanismi (KEM, key encapsulation mechanism). Lyhenne CRYSTALS tulee sanoista ”cryptographic suite for algebraic lattices”. Kyberin turvallisuus perustuu häirityn oppimisen moduliversion ratkaisemisen vaikeuteen, jonka uskotaan kestävän kvanttilaskentaa.

Kyber jakautuu kahteen osaan. Ensimmäinen osa on epäsymmetrinen salausskeema, jossa määritellään avainten generointi, salaus ja salauksen avaamiseen käytettävät algoritmit. Toinen osa on avainten kapselointimekanismiosa, jossa määritellään epäsymmetrisen salausskeeman avulla avainten generointi, avaimen kapselointi sekä avaimen kapseloinnin avaamisalgoritmit.

Työssä tarkastellaan aluksi epäsymmetrisen salausskeeman algoritmeja ja siirrytään sitten avainten kapselointialgoritmeihin.

LEARNING WITH ERRORS

Kyber perustuu Learning with errors (häiritty oppiminen) -ongelmaan, jossa hyökkääjän tulisi arvata salaisuus tuloksista, jotka ovat mahdollisesti väärin.

Häirityn oppimisen ongelma voidaan korkealla tasolla kuvata seuraavasti. Valitaan salaisuus s, jonka kanssa kerrotaan satunnaisia alkioita a. Kertolaskun tulokseen lisätään satunnainen pieni virhe e, jotta tulokset eivät ole aina oikein. Ongelman ratkaisijan tehtävä on löytää salaisuus s pyytämällä satunnaisia alkioita $(a, a \cdot s + e)$ äärellisen monta kappaletta.

ALGORITMIEN SATUNNAISUUS

Kyberin algoritmit on satunnaisia, joten on mahdollista että salattu viesti ei avaudu alkuperäiseksi viestiksi. Tämä on kuitenkin hyvin epätodennäköistä ja tapahtuu todennäköisyydellä 2^-139 tai pienempi.

BUSINESS FINLAND
INSTA
Tampereen yliopisto