PRH Uutisia

Teemakirje kryptogafiasta 4.7.2018

Kryptografiaa, lohkoketjuteknologiaa ja luottamusta EPO:n ja PRH:n yhteisessä seminaarissa

Lohkoketjuteknologiaa on kutsuttu vuoroin vallankumoukselliseksi, mullistavaksi tai tsunamiksi, toisinaan myös kuplaksi. Joka tapauksessa ala on tullut esille, luultavasti jäädäkseen. Samalla sovellettu kryptografia yleisemmin on lohkoketjuteknologiaan perustuvien kryptovaluuttojen muodossa tullut aivan uudella tavalla yleiseen tietoisuuteen.

Julkisten patenttitietokantojen perusteella lohkoketjuteknologia-alan patentointiaktiivisuuden kasvu on ollut lähes eksponentiaalista.

Erityisen suurta kasvu on ollut USA:ssa ja Kiinassa. Näissä maissa toimii myös enin osa alan hakijoista: kiinalaisia yliopistoja ja USA:ssa toimivia startup-yrityksiä sekä pankkeja. Euroopassakin patenttihakemusten määrän kasvu on ollut merkittävää, mutta eurooppalaisia hakijoita on vähän, samoin kuin heille myönnettyjä patentteja.

29.-30.5.2018 EPO:n ja PRH:n yhdessä järjestämässä seminaarissa aiheena olivat kryptografia ja sen sovellukset, erityisesti lohkoketjuteknologiassa.

Lue lisää

Kryptografia ja patentit

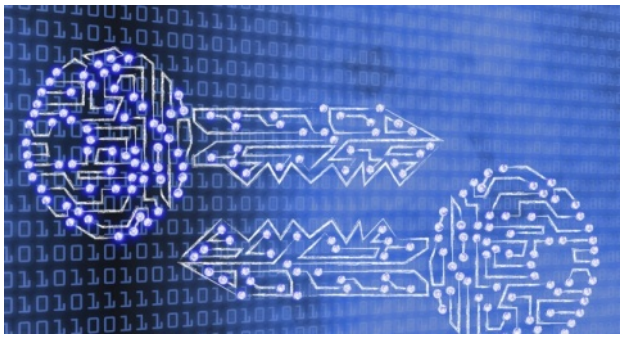
Vaikka jotkut lukuteoreetikot, kuten brittiläinen matemaatikko G.H. Hardy, ovat toisinaan jopa ylpeilleet saavutustensa ”hyödyttömyydestä”, niin vain on käynyt, että muun muassa nykyään niin laajassa käytössä olevat julkisen avaimen salausmenetelmät, kuten monet muutkin kryptografian menetelmät, pohjautuvat lukuteoreettisiin tuloksiin (ja mikäli on uskominen V.I.Arnoldia, Hardylle ominainen huolettomuus ei ole tieteen suurmiehillä edes aivan poikkeuksellista, joskin syyt ovat saattaneet olla vuosisatoja aiemmin erilaiset).

Kryptografian hyödyntämät lukuteorian tulokset koskevat erityisesti alkulukujen ominaisuuksia ja

kokonaislukujen jakamista alkulukutekijöihin. Mutta tästäkin hyödyllisyydestä on vielä matkaa eurooppalaisessa patentoitavuuskäytännössä edellytettävään teknisyyteen.

Lue lisää

Kryptografisten menetelmien teknisyys



Patentin saamista rajoittavat EPC:n artiklan 52(2) rajoitukset koskien matemaattisia menetelmiä sekä suunnitelmia, sääntöjä ja menetelmiä älyllistä toimintaa varten. Näin ollen esimerkiksi klassinen Caesarin salakirjoitus ei olisi patentoitavissa. Laitetta salakirjoituksen tuottamiseksi rajoitus ei tietenkään koske. Caesarin salakirjoituksen automatisointi tietokoneella ei kuitenkaan auttaisi paljoa, koska keksinnöllisyystarkastelussa eroksi yleiskäyttöiseen tietokoneeseen nähden jäisi tuo samainen patentoinnin piiristä pois suljettu menetelmä.

Kuitenkin matemaattinen menetelmä avaimien generoimiseksi julkisen avaimen salakirjoituksessa on teknistä. Näin ollen julkisen avaimen salakirjoituksessa on teknisyyttä, jota Caesarin salakirjoituksessa ei ole. Johtuuko tämä siitä, että julkisen avaimen salakirjoitus on kehittyneempi ja monimutkaisempi kuin Caesarin salakirjoitus vai kenties jostain muusta?

Ei ole niinkään ole kiinnostavaa, olisiko patentin hakeminen edellä mainituissa tapauksissa ollut mielekästä patentointiin liittyvän julkistamisvelvoitteen takia, vaan mikä on innovaatioiden suhde patentin myöntämisen perusteisiin nähden.

Lue lisää

Hajautetut luottamusmekanismit

Lohkoketjuteknologian avulla toisilleen tuntemattomat tahot voivat tuottaa ja ylläpitää erilaisia tietokantoja hajautetusti. Luotetun viranomaistahon sijaan luottamus perustuu konsensusmenettelyllä ennalta määriteltyjen sääntöjen puitteissa tapahtuvaan hyväksymismenettelyyn ja lisäyksien ketjuttamiseen kryptografisten tiivisteiden avulla. Sovellusmahdollisuuksien määrästä saa kuvan ajattelemalla olemassa olevia tietokantaratkaisuja.

Patentoinnin kannalta kiinnostavia kysymyksiä ovat ainakin kysymys siitä, missä määrin lohkoketjut olivat julkistamisvuonna 2008 teknisiltä osiltaan tunnettuja ja missä määrin näiden tunnettujen osien yhdistely ratkaisee teknisen ongelman. Koska keksinnöstä ei tuolloin haettu patenttia, emme tietenkään tiedä täysin vastausta, varsinkin kun keksintöä ei ole muotoiltu patenttivaatimuksena.

Toinen kysymys on, miten lohkoketjuteknologiaa voisi parantaa tai mihin sitä voisi soveltaa siten, että parannus tai sovellutus olisi patentoitavissa.

Lue lisää

Tulevaisuuden näkymiä

Sovellettu kryptografia on lohkoketjuteknologiaan perustuvien kryptovaluuttojen muodossa tullut aivan uudella tavalla yleiseen tietoisuuteen ja patentointiaktiivisuuden kasvu on ollut merkittävää. Myönnettyjä patentteja on kuitenkin Euroopassa vain vähän, ja eurooppalaisten yritysten aktiivisuus maailmanlaajuisesti on ollut pientä. Onko Eurooppa jäämässä jälkeen tärkeällä läpimurtoalalla?

Entä mikä on eurooppalaisen patentointikäytännön mukautumiskyky muutoksien edessä? Vertailukohdaksi voidaan ottaa eurooppalaisen patentoitavuuskäytännön muutokset esimerkiksi matemaattiseen mallinnukseen ja simulointiin liittyvien keksintöjen kohdalla. Mikä muutoksen lopulta aiheutti? Miksi simulointi olisi tänään teknisempää kuin mitä se oli vielä 20 vuotta sitten? Entä voisiko joidenkin muiden alojen asema olla muuttumassa vastaavalla tavalla?

Lue lisää

PIKALINKIT

Kaupparekisteri LEI-tunnus Yhdistykset Säätiöt Yrityskiinnitykset Tilintarkastusvalvonta
Tavaramerkit Mallioikeudet Patentit Hyödyllisyysmallit Tekijänoikeudet Tietoa PRH:sta

PRH Facebookissa PRH Twitterissä PRH Youtubessa

Patentti- ja rekisterihallitus Sörnäisten rantatie 13 C Helsinki I Postiosoite: 00091 PRH
Asiakaspalvelu: Avoinna ma-pe klo 9.00-16.15 I puh. 029 509 5050 I www.prh.fi