Kvanttiturvallisten hilasalausmenetelmien analyysi ja verifiointi

Aalto University
School of Science

MATINE #2500M-0147 02/2022—12/2023

MATINE-tutkimusseminaari 16.11.2023

Estuardo Alpirez Bock, Chris Brzuska, Camilla Hollanti, Rahinatou Njah, Kirthivaasan Puniamurthy, Pavlo Yatsyna

Motivaatio
Tietoturvallisuus/kryptografia

Kvanttitietokoneen muodostama uhka (on täällä jo!)

Merkittävä osa klassisista turvallisuusmekanismeista kaatumassa!

~~RSA~~

~~Diffie-Hellmann~~

Kryptografian perusteita

Symmetrinen vs julkinen avain

- Symmetrinen avain: sekä salaus että salauksen purku tapahtuvat saman salaisen avaimen avulla.
  - Ongelma: miten salainen avain jaetaan turvattoman viestintäkanavan yli?
  - Bonus: avaimen koko pieni.
- Julkinen avain: salaus tapahtuu yleisesti tiedossa olevalla julkisella avaimella. Salauksen purku tapahtuu yksityisellä salaisella avaimella.
  - Bonus: yksityistä avainta ei tarvitse lähettää turvattoman viestintäkanavan yli, vaan se voidaan luoda paikallisesti julkisen avaimen avulla.
  - Ongelma: avaimen koko suuri.

Kryptografian perusteita

Avainkapselointi (Key Encapsulation Mechanism — KEM)

—> **Avainkapselointi:** Käytetään julkisen avaimen systeemiä salaisen avaimen “kapselointiin”. Kun avain on vaihdettu, voidaan käyttää symmetristä systeemiä.

Kvanttiaikakausi:

-tarvitaan tuplakokoisia avaimia symmetrisiin systeemeihin **~OK…**

-julkisen avaimen systeemit/KEM **~???** **—>** **NIST-standardikilpailu**

Kvanttiturvalliset salausmenetelmät

Hilaperusteiset systeemit (LBC)

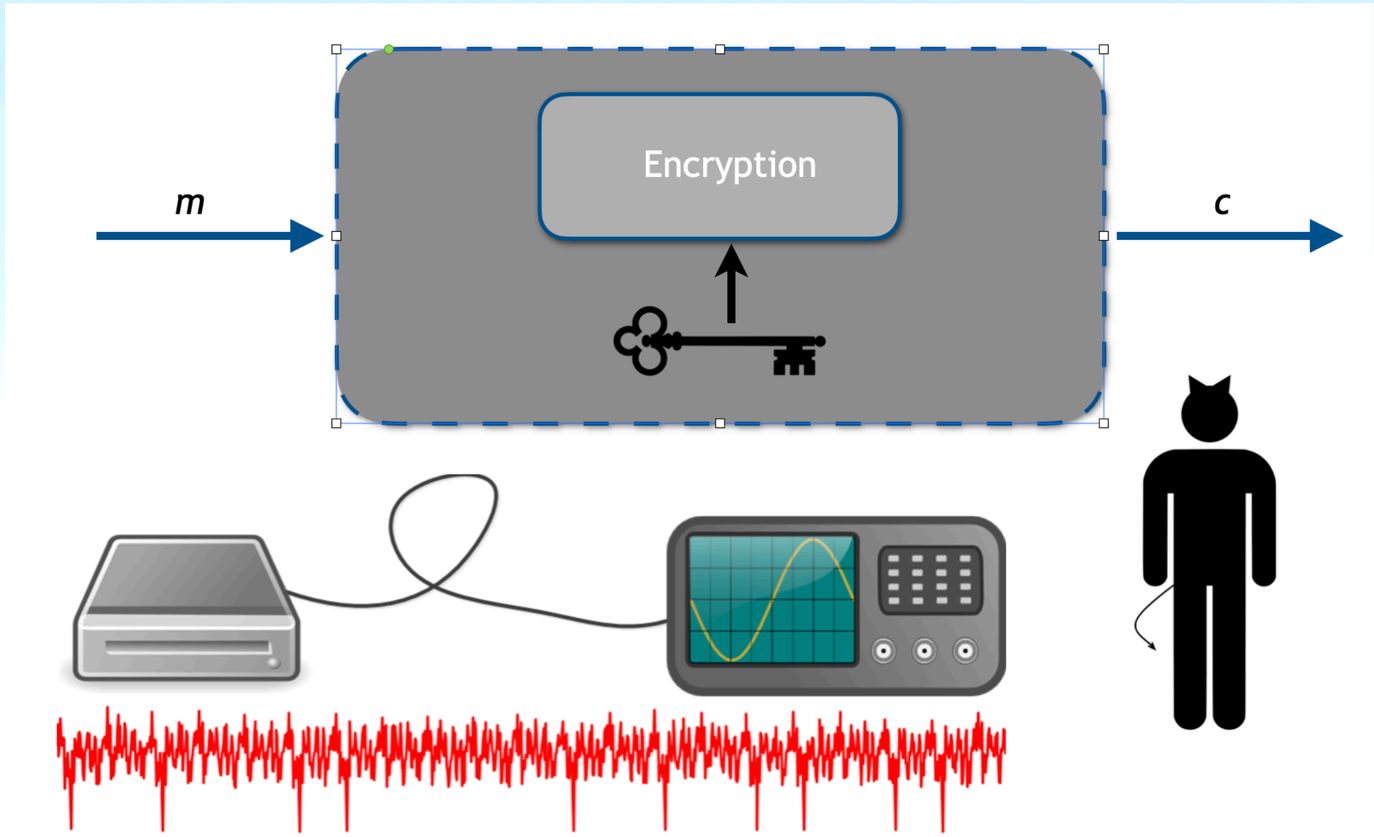
- Kolmen kierroksen jälkeen ainoa standardiin valittu KEM on hilapohjainen (CRYSTALS-Kyber), samoin 2/3 valituista allekirjoitussysteemeistä.
- Projektimme tavoite on analysoida hilapohjaisia kandidaatteja, erityisesti CRYSTALS-Kyber-systeemiä.
- Verifioimme algoritmien turvallisuutta erityisesti sivukanavahyökkäyksissä (SCA).
- Teoreettisempi tutkimuksemme liittyy “kiinnostavien” lukuteoreettisten hilojen ja/tai polynomirenkaiden etsimiseen:

—> löytyy hyökkäys (voidaanko kiertää?)
—> ei tunneta hyökkäystä (mikä on vaikea ongelma?)

Sivukanavahyökkäykset

Kohdistuvat järjestelmän fyysiseen toteutukseen

- Tehonkulutus
- Sähkömagneettinen vuoto
- Tiedon synkronointi
- Ajankäyttö



Hilaperusteiset kryptosysteemit

Hila/verkko *L*:

Neliöhilan $\mathbb{Z}^2 \subseteq \mathbb{R}^2$ yleistys
korkeampiin ulottuvuuksiin:

$$L = \{z_1 B_1 + \cdots + z_n B_n \,|\, z_i \in \mathbb{Z}, \langle B_i \rangle = \mathbb{R}^n\}$$

Hilaperusteiset kryptosysteemit

Vaikeat hilaongelmat turvallisuuden takana

- Hilaongelmilla kryptografian kannalta tärkeitä ominaisuuksia:
    - Pahimman tapauksen redusointi keskimääräiseen tapaukseen; jos ongelma on vaikea pahimmassa tapauksessa, se on vaikea myös keskimäärin.
    - Hyvin tunnettu vaikea ongelma: lähimmän hilapisteen haku (CVP) ja tämän approksimoitu versio.
    - Tämä ongelma palautuu hilan lyhimmän vektorin etsimiseen (SVP). SVP:n vaikeus implikoi saman vaikeuden CVP:lle.

Hilaperusteiset kryptosysteemit

Kohinainen oppiminen (LWE)

- n-ulotteinen vektorijoukko $\mathbb{Z}_q^n$, alkiot kokonaislukuja mod q, q tyypillisesti alkulukupotenssi
- Tasaisesti jakautunut satunnainen salaisuus $s \in \mathbb{Z}_q^n$
- Kohinainen oppiminen:
  - (“search”) Etsi s kun on annettu polynomiaalinen määrä näytteitä (a_i, b_i), missä $a_i \in \mathbb{Z}_q^n$ ovat riippumattomia ja tasaisesti jakautuneita, $b_i \approx < a_i, s >$ ja satunnaisvirhe on lähellä nollaa mod q.
  - (“decision”) Erota mitkä parit $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ on valittu satunnaisesti, ja mitkä yllä olevan mallin mukaisesti.

Hilaperusteiset kryptosysteemit
Kohinaisen oppimisen laajennus lukurenkaisiin (RLWE)

- Edellisen joukon sijaan tarkastellaan näytteitä tietyissä lukurenkaissa (RLWE)
    - RLWE on yhtä vaikea kuin SVP ideaalihilassa —> turvallisuus
- Tunnetaan riittäviä (lukuteoreettisia) ehtoja tietyille hyökkäyksille.
    - Ovatko välttämättömiä?
- Tunnetaan myös riittävät ehdot sekä RLWE—PLWE reduktiolle että search—decision reduktiolle.
    - Ovatko välttämättömiä?

Tulokset

- Tilannekatsausraportti NIST/LBC/SCA.
- Sivukanavahyökkäykset Kyberiä vastaan (yhteistyö Brnon yliopiston ja VTT:n kanssa):
    - lähetetty konferenssijulkaisu CRYSTALS-Kyber-hyökkäyksestä (Estuardo, Kirthi, Chris).
- Edistysaskeleita lukuteoreettisessa ymmärryksessä hilojen/renkaiden soveltuvuudesta/hyökkäysalttiudesta, ml. laajennus homomorfiseen kryptaukseen:
    - yksi julkaistu, kaksi lähetettyä ja kaksi työn alla olevaa artikkelia (Rahinatou et al.),
    - ymmärrys tiettyjen hyökkäysten laajentamisesta/kiertämisestä; “resepti” potentiaalisten hilojen konstruoinnille (Pavlo, Camilla).

Sivukanavahyökkäys CRYSTALS-Kyberiä vastaan

- Kryptografit yrittävät pienentää salatekstin kokoa sekä vähentää salaisella avaimella operointia.
- Kyber valitsi keskitien ja suorittaa salaisella avaimella enemmän toimintoja kuin monet muut järjestelmät.
- Sivukanava-analyysi: mittaamme Kyberiä käyttävän laitteen sähkönkulutusta saadaksemme tietoa salaisesta avaimesta.
- Vaikka yleensä yksinkertaiset vastatoimenpiteet riittävät suojaamaan salaista avainta, analyysi paljasti, että Kyberissä suojaus on em. syystä heikompi.
- Laboratoriotestauksessa pystyttiin poimimaan salainen avain jopa toteutuksesta, joka käyttää sivukanavahyökkäyssuojausta.
- Huono uutinen: hyviä vastatoimia hyökkäystä vastaan on vaikea löytää.
- Hyviä uutisia: hyökkäys on melko kallis ja saattaa olla vaikeampi ei-ihanteellisissa olosuhteissa. Tämä avaa mielenkiintoisia ovia jatkotutkimukselle.

Ohjelmistovuoto

Template attack against Kyber [Alpirez Bock et al.]

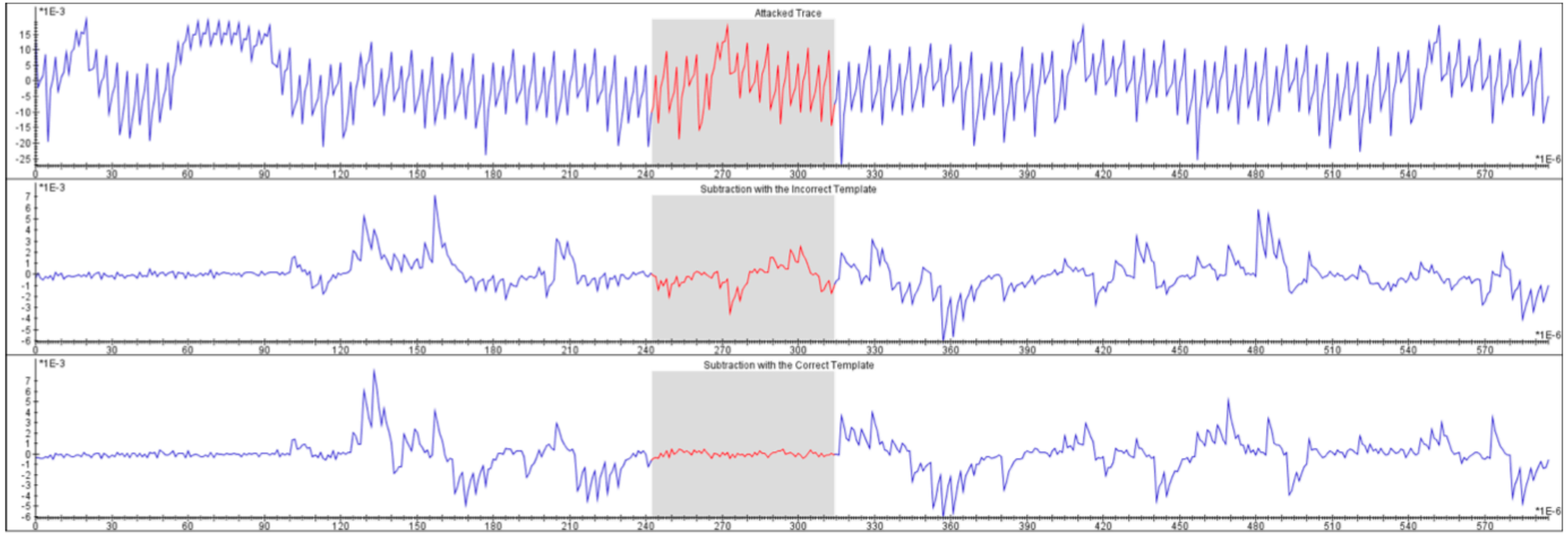


Figure 1: Leakage characterization: target trace with marked pair-point multiplication (top), subtraction of the target trace from an incorrect template (middle), and subtraction of the target trace from the correct template.

RLWE ja lukuteoreettiset hyökkäykset

“Lauter’s list” [El+16]

1. (q) splits completely in K and $q \nmid [R : \mathbb{Z}[x]/(f(x))]$.
2. K is Galois, i.e., all roots of $f(x)$ are in K.
3. $R = \mathbb{Z}[x]/(f(x))$.
4. $f(1) \equiv 0 \pmod{q}$.
5. + some technical (less restrictive) conditions.

- The first three conditions allow for reduction from search to decision and from ring to polynomial LWEs. The fourth condition allows for an attack on P-LWE

—> Täsmennyksiä ja laajennuksia listaan. Uusia ehdokkaita lukurenkaille.

Mitä seuraavaksi?

- Loppuraportin kirjoittaminen.
- Sivukanavahyökkäysten laboratoriotestaus jatkuu yhteistyössä VTT:n kanssa.
- Vierailijaprofessori Ivan Blanco Chacon, U. Alcala Madrid (lukuteoria, hilakrypto) Aallossa 9-12kk 2023–2024. Opinnäytetöiden yhteisohjaus, tutkimusyhteistyö.
- Erityistavoitteet:
    - “Resepti” hyville lukurenkaille (tai muille rakenteille).
    - Lukuteoreettisten hyökkäysten laajennustarkastelu (“huonot” renkaat).
    - Laboratorioverifiointi ja -analyysi.

Viitteet

[Lu+10]: Lyubashevsky V., Peikert C., Regev O., On Ideal Lattices and Learning with Errors over Rings, EUROCRYPT 2010.

[Al+23]: E. Alpirez Bock, G. Banegas, C. Brzuska, L. Chmielewski, K. Puniamurthy, M. Sorf, Breaking DPA-protected Kyber via the pair-pointwise multiplication, https://eprint.iacr.org/2023/551.

[El+16]: Elias, Y., Lauter, K. E., Ozman, E., and Stange, K. E., Ring-LWE Cryptography for the Number Theorist. In Eischen, E. E., Long, L., Pries, R., and Stange, K. E., editors, Directions in Number Theory, pages 271–290, Springer, 2016

[Bl+22]: I. Blanco-Chacón, R. Durán-Díaz, R. Njah Nchiwo, B. Barbero-Lucas, Trace-based cryptanalysis of cyclotomic PLWE for the non-split case, preprint 2022, arXiv:2209.11962

Kiitos!

https://people.aalto.fi/chris.brzuska

http://math.aalto.fi/en/research/discrete/anta/index.html