Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 35 – 52 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

პოსტკვანტური ციფრული ხელმოწერა ვერკლის ხისა და ლატისების გამოყენებით

POST-QUANTUM DIGITAL SIGNATURE USING VERKLE TREES AND LATTICES

Maksim Iavich[1], Tamari Kuchukhidze[1], Avtandil Gagnidze[2]

[1] Department of Computer Science, Caucasus University, 0102, Georgia
[2] East West University, 9 Vakhtang Gorgasali St, Tbilisi

რეზიუმე: ბოლო წლებში კვანტურ კომპიუტერებზე კვლევები მნიშვნელოვნად განვითარდა. თუკი კაცობრიობა ოდესმე შექმნის ეფექტურ კვანტურ კომპიუტერს, არსებული საჯარო გასაღების უმეტესი კრიპტოსისტემებს პრობლემები შეექმნება. ასეთი სახის კრიპტოსისტემები დღსდღეობით გვხვდება ბევრ კომერციულ პროდუქტში. ჩვენ შევიმუშავეთ შედეგები, რომლებიც, ერთი შეხედვით გვიცავს კვანტური შეტევებისგან, მაგრამ ისინი სახიფათო და არაეფექტურია ყოველდღიურ ცხოვრებაში გამოსაყენებლად. ნაშრომში გაანალიზებულია ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის მეთოდები. შეფასებულია მერკლის ხეზე დაფუძნებული ელექტრონული ხელმოწერა. ვერკლის ხის და ვექტორული ვალდებულებების გამოყენებით ნაშრომი იკვლევს ახალ იდეებს.
ამ სტატიაში წარმოვადგენთ უნიკალურ ტექნოლოგიას, პოსტკვანტური ციფრული ხელმოწერის სისტემის შემუშავებისთვის, რომლისთვისაც ვიყენებთ უახლეს ვერკლის ხეს. ამ მიზნისთვის გამოიყენება ვერკლის ხე, ვექტორული ვალდებულებები და ისეთი ვექტორული ვალდებულებები, რომლებიც დაფუძნებულია ლატისებზე, პოსტკვანტური თვისებებისთვის. ნაშრომში ასევე მოცემული პოსტკვანტური ხელმოწერის დიზაინის ცნებები ვერკლის ხის გამოყენებით.

საკვანძო სიტყვები: პოსტ-კვანტური კრიპტოგრაფია; კვანტური კრიპტოგრაფია; გვერდითი არხის თავდასხმები; CRYSTALS-Kyber; მასკირება; ღრმა სწავლება; ლატისებზე დაფუძნებული კრიპტოგრაფია.

ABSTRACT: Significant advancements have been achieved in the field of quantum computing in recent years. If somebody ever create a sufficiently strong quantum computer, many of the public key cryptosystems in use today might be compromised. Kyber is a post-quantum encryption technique that depends on lattice problem hardness, and it was recently standardized. Despite extensive testing by the National Institute of Standards and Technology (NIST), new investigations have demonstrated the effectiveness of Crystals-kyber attacks and their applicability in non-controlled environments.
We investigated CRYSTALS-Kyber's susceptibility to side-channel attacks. In the reference implementation of Kyber512, additional functions can be compromised by employing the selected ciphertext. The implementation of the selected ciphertext allows the attacks to succeed. Real-time recovery of the entire secret key is possible for all assaults.

KEYWORDS: post-quantum cryptography; quantum cryptography; side-channel attacks; CRYSTALS-Kyber; masking; deep-learning; lattice-based cryptography.

1. შესავალი

კვანტური გამოთვლები საბოლოოდ უფრო გავრცელებული გახდება, რაც გამოიწვევს პოსტკვანტური კრიპტოგრაფიის განვითარებას. პოსტკვანტური კრიპტოგრაფია, რომელიც ასევე ცნობილია როგორც კვანტური დაშიფვრა, არის კლასიკური კომპიუტერების დაცვის საშუალება კვანტური კომპიუტერის შეტევებისგან [1]. კვანტურ კომპიუტერებს შეუძლიათ რთული გამოთვლების შესრულება ბევრად უფრო სწრაფად, ვიდრე ჩვეულებრივ დესკტოპ კომპიუტერებს, რასაც შეიძლება წლები დასჭირდეს ჩვეულებრივი კომპიუტერებისთვის. კვანტურმა კომპიუტერმა შეიძლება დაარღვიოს სტანდარტული კრიპტო სისტემების უმეტესობა, თუ არა ყველა, რომელიც ამჟამად ვიყენებთ პრაქტიკაში.

კვანტური გამოთვლის განვითარებისას, უფრო საგულისხმო ხდება კრიპტოგრაფიის მიმდინარე მეთოდების ეფექტურობა. იგულისხმება გავრცელებული მეთოდები, როგორიცაა RSA ან ელიფსური მრუდის კრიპტოგრაფია (ECC). RSA-ს უსაფრთხოება ეყრდნობა რთულ მათემატიკურ ამოცანებს, როგორიცაა მთელი რიცხვების ფაქტორიზაცია. კვანტურ გამოთვლას, შორის ალგორითმის მსგავსი ტექნიკის გამოყენებით, შეუძლია ამ პრობლემების გადაჭრა, რაც მნიშვნელოვან საფრთხეს უქმნის RSA-ს [2], შესაბამისად ყველა სისტემას რომლებიც RSA–ზე არის დაფუძნებული. ეს არის ერთ–ერთი მაგალითი არსებული მეთოდების არაეფექტურობის.

კვანტური გამოთვლების ზრდა გვიჩვენებს, რომ დაშიფვრის ტრადიციული მეთოდები შეიძლება მოძველდეს. ამან განაპირობა მონაცემთა დაცვის ახალი მეთოდების შემუშავება, როგორიცაა ლატისებზე დაფუძნებული დაშიფვრა, რომელიც შექმნილია კვანტური კომპიუტერის შეტევების წინააღმდეგობის გასაწევად [3].

ამ სირთულის გაცნობიერებით, პოსტ-კვანტური კრიპტოსისტემები, რომლებსაც შეუძლიათ უსაფრთხოდ და წარმატებით გაუძლონ კვანტურ შეტევებს, უნდა განვავითაროთ და გამოვიყენოთ [4–5]. კვანტური გამოთვლების სრულყოფის შემთხვევაში, ჩვეულებრივი ასიმეტრიული მეთოდები, როგორიცაა RSA, ვერ იქნება ადეკვატური პირადი მონაცემების დასაცავად. კვანტური ტექნოლოგიების განვითარების შედეგად აუცილებელი გახდა მუდმივად შევქმნათ და განვავითაროთ მოქნილი პოსტკვანტური სისტემები [6].

არსებული კვანტური კომპიუტერული საფრთხის მოსაგვარებლად, სტანდარტებისა და ტექნოლოგიების ეროვნულმა ინსტიტუტმა (NIST)–მა 2016 წელს დაიწყო პოსტ-კვანტური კრიპტოგრაფიის სტანდარტიზაციის ინიციატივა (NIST PQC). მისი მიზანია შეიქმნას ძლიერი კრიპტოგრაფიული სტანდარტები, რომლებიც შეძლებენ წინააღმდეგობა გაუწიონ კვანტურ კომპიუტერულ შეტევებს და უზრუნველყონ მგრძნობიარე მონაცემები.

NIST–მა ეს პროცესი დაიწყო კრიპტოგრაფიის საზოგადოების მიერ წარმოდგენილი პოტენციური ალგორითმების ჯგუფების შერჩევით. ეს ალგორითმები ფართოდ გამოიცადა კვანტური შეტევების მიმართ, როგორი გაუძლებდნენ. ბოლო სტადიებში გადავიდა

ალგორითმები, რომლებიც ეფუძნება რთულ მათემატიკურ ამოცანებს, როგორიცაა წრფივი შეცდომის გამოსწორების კოდის დეკოდირება (linear error-correcting code decoding) და ლატისები, რომელთა გადაჭრა ძნელია კვანტური კომპიუტერებისთვის.

2022 წლის ივლისში NIST-მა 2022 გამოაცხადა, რომ CRYSTALS-Kyber გახდება ახალი სტანდარტი გასაღების პარამეტრების და საჯარო გასაღების დაშიფვრისთვის (PKE) [7]. ეს არის მთავარი. ამ არჩევანის მიზეზი არის ის, რომ იგი იდენტიფიცირებულია, როგორც ძირითადი ინკაფსულაციის მექანიზმი (KEM), რომელიც უზრუნველყოფს IND-CCA2 შემთხვევით ორაკულების მოდელებში, რომლებიც არის როგორც კლასიკური, ასევე კვანტური. შეცდომებით სწავლის მოდულის სირთულე (M-LWE), რომელიც ხაზს უსვამს უცნობ ხმაურს, ქმნის CRYSTALS-Kyber-ის უსაფრთხოების საფუძველს. გარდა ამისა, CRYSTALS-Kyber სწრაფად ჩართეს ეროვნული უსაფრთხოების სააგენტოს (NSA) მიერ ეროვნული უსაფრთხოების აპლიკაციებისთვის შემოთავაზებული კრიპტოგრაფიული ალგორითმების კოლექციაში [8]. ეს ხაზს უსვამს ალგორითმის მნიშვნელობას კრიპტოგრაფიული სისტემების დაცვაში ახალი კვანტური საფრთხეებისგან.

ცნობილია თავისი IND-CCA2 უსაფრთხოებით, მისი გამოვლენა შეუძლებელია ადაპტური შერჩეული შიფრული ტექსტის შეტევის დროს [9]. იმის გამო, რომ ის შეიცავს უცნობი ხმაურის ჩასმას წრფივ განტოლებებში, მოდულის სწავლა შეცდომებით (M-LWE) პრობლემა რთულია, რაც განსაზღვრავს/უზრუნველყოფს მის უსაფრთხოებას.

CRYSTALS-Kyber და სხვა პოსტკვანტური დაშიფვრის ალგორითმების ცნობილი სისუსტეებია დაცულ პროგრამული უზრუნველყოფის დანერგვაში. გვერდითი არხის ანალიზის მოწინავე მეთოდებმა, განსაკუთრებით ღრმა სწავლის გამოყენებით, შეძლეს ამ განხორციელებების დარღვევა. ამ მოწყვლადობამ განაპირობა უკეთესი დაცვის განვითარება და CRYSTALS-Kyber-ის გაუმჯობესებული დანერგვა.

მნიშვნელოვანია შევაფასოთ რამდენად კარგად ეწინააღმდეგება CRYSTALS-Kyber-ის დანერგვა გვერდითი არხის თავდასხმებს. ეს შეტევები იყენებს არაპირდაპირ, დაკვირვებადი არხების ინფორმაციას, როგორიცაა დრო ან ელექტროენერგიის მოხმარება და სერიოზულ საფრთხეს უქმნის კრიპტოგრაფიულ უსაფრთხოებას.

Kocher et al. [10] მიაღწია მნიშვნელოვან წინსვლას ამ სფეროში დიფერენციალური გვერდითი არხის ანალიზის შემუშავებით, რომელიც იყენებდა ფიზიკურ მონაცემებში განსხვავებებს. ღრმა სწავლაზე დაფუძნებული გვერდითი არხის ანალიზი [11] იყო კიდევ ერთი მნიშვნელოვანი განვითარება, რამაც შესაძლებლობა მოგვცა თავდასხმების განხორციელება მომხდარიყო სხვადასხვა კრიპტოგრაფიულ სისტემაზე. ტრადიციული თავდაცვა ვერ უძლებს ამ თავდასხმებს. არანაკლებ მნიშვნელოვანია, Wang et al.-ის [12] შეცდომის ინექციის მეთოდი, რომელიც არღვევს რთულ სამიზნეებს, როგორიცაა CRYSTALS-Kyber-ის ტექნიკის დანერგვა არადიფერენციალური თავდასხმების დიფერენციალურზე გარდაქმნით.

ბევრი საპირისპირო ღონისძიება, კონტრზომა არსებობს, მათ შორის, დაფარვა/მასკირება [13-15], არევა [16-18], რანდომიზებული საათი [19-20], შემთხვევითი შეფერხებების ჩასმა [21-23], მუდმივი წონის დაშიფვრა [24] და კოდის პოლიმორფიზმი [25- 26], გამოიყენება გვერდითი

არხის თავდასხმების შესამცირებლად. ინფორმაციის გაჟონვის თავიდან ასაცილებლად ფიზიკურად რაოდენობრივი არხებით, როგორიცაა დრო [27–28], ენერგიის მოხმარება [29–30] ან ელექტრომაგნიტური გამოსხივება [31–32], ეს კონტრზომები კრიპტოგრაფიული სისტემების დაცვას ცდილობს.

საბოლოოდ, გვერდითი არხის თავდასხმები (side-channel attacks) უფრო დახვეწილი ხდება, რაც ხაზს უსვამს კრიპტოგრაფიული განხორციელების უსაფრთხოების მუდმივი შეფასების და გაუმჯობესების მნიშვნელობას - განსაკუთრებით მაშინ, როდესაც საქმე ეხება პოსტკვანტურ კრიპტოგრაფიის ალგორითმებს, როგორიცაა CRYSTALS-Kyber.

2. კიბერის და CRYSTALS-კიბერის მიმოხილვა

კიბერი (Kyber) არის უსაფრთხო გასაღების ინკაფსულაციის მექანიზმი (KEM), რომელიც დაფუძნებულია შეცდომებთან სწავლის (LWE) პრობლემაზე, რომელიც იყენებს ლატისების მოდულს. ეს არის NIST–ის პოსტ-კვანტური კრიპტოგრაფიის პროექტის ერთ-ერთი კანდიდატი. წინადადებაში შედის სამი პარამეტრის ნაკრები, უსაფრთხოების სხვადასხვა დონისთვის: Kyber-512 (მსგავსი AES-128–ის), Kyber-768 (მსგავსი AES-192–ის) და Kyber-1024 (მსგავსი AES-256–ის).

რეკომენდებულია კიბერის გამოყენება ჰიბრიდულ რეჟიმში, მისი ინტეგრირება უსაფრთხოების ცნობილ „წინასწარ კვანტურ“ პროცედურებთან. დიფი-ჰელმანის გაერთიანება ელიფსურ მრუდთან არის ერთი–ერთი კონკრეტული მაგალითი. ეს მეთოდი იყენებს როგორც პოსტკვანტური, ასევე კლასიკური კრიპტოგრაფიის უპირატესობებს [33].

მიზანშეწონილია გამოვიყენოთ Kyber-768 პარამეტრის ნაკრები. ეს პარამეტრის შერჩევა გვთავაზობს 128 ბიტზე მეტ უსაფრთხოებას ყველა ცნობილი ჩვეულებრივი თუ კვანტური შეტევის წინააღმდეგ. ეს მიღებულია კონსერვატიული ანალიზის მიხედვით, რომელმაც მიიღო ეს გადაწყვეტილება. კრიპტოგრაფიის სამყაროში, 128 ბიტიანი უსაფრთხოება განიხილება, როგორც უკიდურესად ძლიერი და მდგრადი, როგორც ცნობილი, ისე უცნობი საფრთხეების მიმართ.

2022 წლის ზაფხულში, NIST-მა (აშშ-ის სტანდარტებისა და ტექნოლოგიების ეროვნულმა ინსტიტუტმა) სტანდარტიზაციისთვის შეარჩია CRYSTALS-Kyber, კვანტურად უსაფრთხო გასაღების კაფსულაციის ახალი მეთოდი. CRYSTALS ნიშნავს კრიპტოგრაფიულ კომპლექტს ალგებრული ლატისებისთვის.

Kyber არის CCA-უსაფრთხო KEM სქემა, რომელიც არის CRYSTALS-Kyber-ის ნაწილი. შერჩეული ღია ტექსტის თავდასხმის (CPA) უსაფრთხო PKE ტექნიკაზე დაშენებულია კიბერი, აგებულია CCAKEM.CPAPKE (სურათები 1 და 2), სადაც გამოვიყენებთ Fujisaki-Okamoto (FO) ტრანსფორმაციის მორგებული ვერსიას [34].

CPAPKE.KeyGen()

seed $_A \leftarrow \mathcal{U}(\{0,1\}^{256})$

$A \leftarrow \mathcal{U}\left(R_q^{k\times k}; seed_A\right)$
$s \leftarrow \mathcal{B}_{\eta_1}\left(R_q^{k\times 1}\right)$
$e \leftarrow \mathcal{B}_{\eta_1}\left(R_q^{k\times 1}\right)$
$b = As + e_{p_1}$
$pk = (seed_A, b), sk = s$
return (pk, sk)

CPAPKE. Enc$(pk = (seed_A, b), m, r)$

$A \leftarrow \mathcal{U}\left(R_q^{k\times k}; seed_A\right)$
$s' \leftarrow \mathcal{B}_{\eta_1}\left(R_\eta^{k\times 1}; r\right)$
$e' \leftarrow \mathcal{B}_{\eta_2}\left(R_q^{k\times 1}; r\right)$
$e'' \leftarrow \mathcal{B}_{\eta_2}\left(R_q^{1\times 1}; r\right)$
$u = \lfloor (As' + e') \cdot 2^{d_u}/q \rceil$
$v = [(b \cdot s' + e'' + encode(m)) \cdot 2^{d_v}/q]$
return $c = (u, v)$

CPAPKE.Dec(s, $c = (u, v)$)

$y = \lfloor v \cdot q/2^{d_v} \rceil - s\lfloor u \cdot q/2^{d_u} \rceil$
$m' = decode(y)$
return m'

ფიგურა 1. CCAPKE ალგორითმები

Kyber.KeyGen()

$z \leftarrow \mathcal{U}(\{0,1\}^{256})$

$(pk, \mathrm{s}) = \mathrm{CPAPKE.KeyGen()}$

$sk = (\mathrm{s}, pk, \mathcal{H}(pk), z)$

return (pk, sk)

Kyber.Encaps (pk)

$m \leftarrow \mathcal{U}(\{0,1\}^{256})$

$(\hat{K}, r) = \mathcal{G}(m, \mathcal{H}(pk))$

$c = \mathrm{CPAPKE.\,Enc}(pk, m, r)$

$K = \mathrm{KDF}(\hat{K}, \mathcal{H}(c))$

return (c, K)

Kyber.Decaps $(sk = (\mathbf{s}, pk, \mathcal{H}(pk), z), c)$

$m' = \mathrm{CPAPKE.Dec}(\mathrm{s}, c)$

$(\hat{K}', r') = \mathcal{G}(m', \mathcal{H}(pk))$
$d' = \mathrm{CPAPKE.Enc}\ (pk, m', r')$
if $c = c'$ then

return $K = \mathrm{KDF}(\hat{K}, \mathcal{H}(c))$

else

return $K = \mathrm{KDF}\left(z, \mathcal{H}(c)\right)$

end if

ფიგურა 2. CCAPKE ალგორითმები

CRYSTALS-Kyber იყენებს რგოლის (ring) ელემენტების ვექტორებს R_q^k-ში, სადაც k არის მოდულის რანგი, რომელიც გამოიყენება უსაფრთხოების დონის გასაზომად. CRYSTALS–Kyber-ის შემთხვევაში გვაქვს სამი განსხვავებული ვარიანტი k=2, 3 და 4-ისთვის, Kyber-512, Kyber-768 და Kyber-1024. ვინაიდან მისაღები იმპლემენტაცია მხარს უჭერს Kyber-512-ს, ეს ვერსია არის მთავარი აქცენტი. რიცხვთა თეორიული ტრანსფორმაცია (NTT) გამოიყენება CRYSTALS-Kyber-ის მიერ R_q-ში გამრავლების ეფექტურად შესასრულებლად.

მნიშვნელობა K იქმნება შეტყობინებისა და საჯარო გასაღების ჰეშის კომბინაციით, CPAPKE.Enc ფუნქციის გამომავალი ჰეშთან, გასაღების გენერაციის ფუნქციის გამოყენებით. ეს ნიშნავს, რომ დაშიფვრის გასაღები (K) მომდინარეობს შეტყობინების, საჯარო გასაღებისა და დაშიფვრის ფუნქციის (CPAPKE.Enc) დამატებითი მონაცემებიდან. ეს პროცესი აღწერილია Kyber.Encaps ფუნქციაში, სადაც K იქმნება დაშიფვრის დროს და ხდება მისი დაბრუნება. გაშიფვრის შემდეგ (Kyber.Decaps), K შეიძლება იყოს იგივე, რაც დაშიფვრის დროს ან იქნება ყალბი მნიშვნელობა, რაც დამოკიდებულია დაშიფრული ტექსტის მთლიანობაზე. შემავალი მნიშვნელობა r, რომელიც არის CPAPKE.Enc-ისთვის, მიღებულია შეტყობინებისა და საჯარო გასაღების ჰეშირებიდან, ვიდრე თვითნებური მნიშვნელობის გამოყენებით, უსაფრთხოების გასაძლიერებლად.

შეცდომებზე დაფუძნებული სწავლის სქემებს (Error-Based Learning schemes), როგორიცაა კიბერი, შეიძლება ჰქონდეს გაშიფვრის წარუმატებლობები, რაც თავდამსხმელებმა შესაძლოა გამოიყენონ პირადი ინფორმაციის აღმოსაჩენად. ეს წარუმატებლობა უფრო სავარაუდოა, თუ თავდამსხმელები ქმნიან საიდუმლო ვექტორებს და შეცდომის მნიშვნელობებს CPAPKE.Enc-ში დაშვებული ლიმიტებს მიღმა.

Kyber.Encaps და Kyber.Decaps იყენებენ შეცვლილ Fujisaki-Okamoto-ს ტრანსფორმაციას, რათა უზრუნველყონ შემთხვევითი საიდუმლოების და შეცდომის მნიშვნელობები დაგენერირდეს სწორად და კარგად იყოს დამოწმებული გაშიფვრის დროს.

CRYSTALS-Kyber ალგორითმი იყენებს Fujisaki-Okamoto (FO) ტრანსფორმაციას CCA2 უსაფრთხოების უზრუნველსაყოფად. პირველ რიგში ის დაშიფრულ ტექსტის დეშიფრაციას ახდენს CPA-ის გამოყენებით. შემდეგ ის „ხელახლა დაშიფრავს“ შეტყობინებას ახალი დაშიფრული ტექსტის c' მისაღებად. ამოწმებს, შეესაბამება თუ არა c' თავდაპირველ დაშიფრულ ტექსტს c–ს. თუ ისინი ემთხვევა, შედეგი არის სწორი (True); წინააღმდეგ შემთხვევაში, შედეგი მცდარია (False). სესიის გასაღების K წარმოქმნა დამოკიდებულია ამ შედეგზე. FO ტრანსფორმაცია ხელს გვიწყობს აღმოვაჩინოთ თავდამსხმელის მიერ განხორციელებული ნებისმიერი ცვლილება.

არსებითად ეს კიბერ მექანიზმი გვიცავს თავდამსხმელებისგან, რომლებიც იყენებენ სისუსტეებს დაშიფვრისა და გაშიფვრის პროცესებში. ის განიხილავს პოტენციურ საკითხებს, რომლებიც დაკავშირებულია გაშიფვრის წარუმატებლებთან შეცდომებთან სწავლების სქემებში.

3. გვერდითი არხის თავდასხმები

კრიპტოგრაფიული სისტემები შეიძლება უსაფრთხოდ გამოიყურებოდეს მათემატიკური შეტევებისგან, მაგრამ მაინც არ არიან დაცული გვერდითი არხის თავდასხმებისგან. ამ სტილის შეტევები იყენებენ სისტემების მუშაობის დროს განმავლობაში გაჟონულ მონაცემებს, როგორიცაა ელექტრომაგნიტური გამოსხივება, ხმის ტალღები, ენერგიის მოხმარება ან შესრულების დრო [35]. პირველად გამოვლინდა პოლ კოჩერის მიერ 1996 წელს, გვერდითი არხის თავდასხმები განსაკუთრებით სარისკოა ჩაშენებული სისტემებისთვის. მიუხედავად იმისა, რომ პოსტ-კვანტური კრიპტოგრაფიის (PQC) ბევრი კანდიდატი წინააღმდეგობას უწევს მარტივ დროით შეტევებს, სხვა გვერდითი არხის შეტევების მეთოდებს, როგორიცაა სიმძლავრე და ელექტრომაგნიტური ანალიზი, კვლავ შეუძლიათ საფრთხე შეუქმნან სისტემებს. მკვლევარები მუშაობენ ამ მოწყვლადობის იდენტიფიცირებასა და შერბილებაზე. NIST ხაზს უსვამს გვერდითი არხის თავდასხმებზე წინააღმდეგობის მნიშვნელობას PQC დანერგვაში, რომ ვუზრუნველყოთ ჩვენი სისტემების უსაფრთხოება.

მეცნიერებმა ჩაატარეს საფუძვლიანი გამოკვლევა იმის შესახებ, თუ რამდენად მგრძნობიარეა ლატისებზე დაფუძნებული გასაღების ინკაფსულაციის მექანიზმები (KEM) სხვადასხვა გვერდითი არხის შეტევების მიმართ. მკვლევარებმა ყურადღება გაამახვილეს გვერდითი არხის დახმარებით შერჩეულ დაშიფრული ტექსტის შეტევებზე (CCA), რომლებიც მიზნად ისახავს საიდუმლო გასაღების მოპოვებას ლატისებზე დაფუძნებული გასაღების ინკაფსულაციის მექანიზმებში (KEM) [36-37]. ეს შეტევები მიზნად ისახავს სხვადასხვა პროცესებს, როგორიცაა Fujisaki-Okamoto (FO) ტრანსფორმაცია, შეტყობინების კოდირება/გაშიფვრა, ინვერსიული რიცხვის თეორიული ტრანსფორმაცია (NTT) და შეცდომების გამოსწორების კოდები. გვერდითი არხის თავდასხმები იყენებს არაპირდაპირ არხებს, როგორიცაა დრო ან ენერგიის მოხმარება. კრიპტოგრაფიული ოპერაციების დროს ელექტრო სიგნალებში დაუცველობის დასადგენად, მკვლევარებმა გამოიყენეს ვერტიკალური გვერდითი არხის გაჟონვის გამოვლენა CRYSTALS-Kyber-ის გაშიფვრის პროცესის გასაანალიზებლად.

KYBER-512-ს აქვს ხარვეზები, რომლებიც თავდამსხმელს საშუალებას აძლევს აღადგინოს გასაღები რამდენიმე მარტივი მოთხოვნით, თუკი შემტევმა იცის გაშიფრული შეტყობინებები [38]. ეს შეტევები ფოკუსირებულია შეტყობინების დაშიფვრაზე და ინვერსიულ რიცხვთა თეორიულ ტრანსფორმაციაზე (NTT) სუფთა და m4 სქემებში. m4 სქემა არის Kyber-ის ოპტიმიზებული ვერსია ARM Cortex-M4 CPU-სთვის, რომელიც შედის pqm4 ბიბლიოთეკაში. საიდუმლო გასაღების აღდგენა შესაძლებელია მხოლოდ ოთხი ძიებით თუ საქმე გვაქვს სუფთა სქემასთან და რვა ძიებით შეგვიძლია აღვადგინოთ m4 სქემის შემთხვევაში.

ასევე გვაქვს შეტყობინებების აღდგენის მეთოდები, როგორიცაა შეტყობინებების ციკლური როტაცია და მიზნობრივი ბიტის შებრუნება [39]. ეს მეთოდები მოითხოვს (w + 1) ნაკვალევს (traces) გვერდითი არხის ჰემინგის წონის კლასიფიკატორით. საწინააღმდეგო ზომებით მასკირებისა და არევის/შერწყმის მიუხედავად, აპლიკაციები შესაძლოა მაინც დაუცველი

იყოს. თუმცა, ამ კონტრზომებით დაცულ იმპლემენტაციებზე თავდასხმა მოითხოვს, რომ თავდამსხმელმა შეძლოს მათი დეაქტივაცია შაბლონების შესაქმნელად.

გარდა ამისა, მკვლევარებმა შემოგვთავაზეს აღდგენილ შეტყობინებებზე დაფუძნებული გასაღების აღდგენის შეტევა, რომელსაც დასჭირდება ექვსი კონკრეტული დაშიფრული ტექსტი. მნიშვნელოვანია გვახსოვდეს, რომ KYBER-512 ხმაურის მნიშვნელობა გაიზარდა და CRYSTALS-კიბერის სპეციფიკაცია შეიცვალა, რაც მიუთითებს იმაზე, რომ ახლა საჭიროა უფრო ფრთხილად მომზადებული დაშიფრული ტექსტები [40].

4. მასკირება

მასკირების გამოყენებით ვცდილობთ CRYSTALS-Kyber დავიცვათ გვერდითი არხის თავდასხმებისგან. კრიპტოგრაფიული ალგორითმების არითმეტიკული ქცევის დამალვის მიზნით, საპირისპირო ღონისძიება, რომელიც ცნობილია როგორც მასკირება/შენიღბვა მოიცავს საიდუმლოების დაყოფას ბევრ, ნაწილობრივ რანდომიზებულ აქციებად (სადაც მეხუთე რიგი ეხება საიდუმლო გაყოფას ხუთჯერ). ჩვენ გამოვიყენებთ ტექნიკას სახელწოდებით masking, რათა გავაძლიეროთ CRYSTALS-Kyber გვერდითი არხის შეტევებისგან [41].

სიმძლავრისა და ელექტრომაგნიტური გვერდითი არხის გამოკვლევის ზოგადი დაცვა არის მასკირება. ფუნდამენტურად, მასკირება გულისხმობს ფარული მნიშვნელობის დაყოფას რამდენიმე ნაწილად შემთხვევით. ალგორითმი თითოეულ ეტაპზე დამოუკიდებლად ამუშავებს ამ დაყოფილ ინფორმაციას, აერთიანებს შედეგებს საბოლოო სასურველი შედეგის მისაღებად. დაფარვის დომენის შიგნით მუშაობა აჩერებს x ცვლადის მგრძნობიარე ინფორმაციის გაჟონვას, რადგან ის არასოდეს გამოიყენება პირდაპირ. ესე იგი, პირდაპირ ერთიან ინფორმაციას არ ვიყენებთ. ეს მთლიანი იყოფა რამდენიმე ნაწილად. მგრძნობიარე ცვლადი x იყოფა $\omega + 1$ ნაწილად, ეს არის ω - რიგის შენიღბვა. ვიღებთ $x = x_1 \circ x_2 \circ \dots \circ x_{\omega+1}$, ისე რომ $x = x_1 \circ x_2 \circ \dots \circ x_{\omega+1}$. გვაქვს მასკირების ორი: არითმეტიკული და ლოგიკური (Arithmetic and Boolean) ვარიანტი. შენიღბვის ტექნიკიდან გამომდინარე, "∘" შეიძლება წარმოადგენდეს სხვადასხვა ოპერაციებს. მაგალითად, არითმეტიკული მასკირებისას "∘" არის არითმეტიკული დამატება, ხოლო ლოგიკური მასკირების დროს ეს არის XOR.

გამოთვლების შემთხვევაში ვცდილობთ თავიდან ავიცილოთ საწყისი ინფორმაციის x – ის პირდაპირ გამოყენებას. ოპერაციებზე მოქმედებები სრულდება სხვადასხვა ნაწილებზე დამოუკიდებლად, რაც თეორიულად ხელს უშლის x-ის შესახებ გვერდითი არხის საშუალებებით ინფორმაციის გაჟონვას. ყოველ ჯერზე, როდესაც ვყოფთ ინფორმაციას, ის შემთხვევით არის არჩეული. რანდომიზაცია ჩვეულებრივ მიიღწევა შემთხვევითი მასკირების $x_1, x_2, \dots, x_\omega$ გადანაწილებით ω წილებზე და საბოლოო ნაწილი ანგარიშდება შემდეგნაირად: $x - (x_1 + x_2 + \cdots + x_\omega)$ არითმეტიკული ნიღბისთვის ან თუკი ლოგიკურ მასკირებასთან გვაქვს საქმე ამ წესით $x \oplus x_1 \oplus x_2 \oplus \dots \oplus x_\omega$. [42].

5. კიბერის უახლესი იმპლემენტაცია

კიბერის პოსტ-კვანტური კრიპტოგრაფიის ალგორითმმა, რომელიც რეკომენდირებულია NIST-ის მიერ, მნიშვნელოვანი პროგრესი განიცადა დანერგვის პროცესში. უახლესი კვლევები მიზნად ისახავს კიბერის მუშაობისა და ეფექტურობის გაუმჯობესებას ინოვაციური აპარატიული (hardware) დიზაინის გამოყენებით.

კვლევებმა შემოიტანა სპეციალური მოწყობილობები, აპარატურის ამაჩქარებლები და FPGA დანერგვები [43] პოლინომიური ოპერაციებისა და მოდულარული არითმეტიკის დასაჩქარებლად. ისინი გადამწყვეტია კიბერის დაშიფვრისა და გაშიფვრისთვის. ერთ–ერთი მაგალითია CRYPHTOR არქიტექტურა, რომელიც მოიცავს სპეციფიკურ ALU-ებს და მეხსიერების კონფიგურაციებს კიბერისა და Dilithium ალგორითმებისთვის [44]. CRYPHTOR ინტეგრირებულია 64-ბიტიან და 32-ბიტიან RISC-V-ზე დაფუძნებულ სისტემებში ჩიპზე (SoCs), რაც ძალიან დიდ სისწრაფეს აღწევს: 26-მდე რიცხვის თეორიული ტრანსფორმაციის (NTT) ოპერაციებისთვის და 140-მდე მატრიცა-ვექტორის ნამრავლისას.

FPGA-ის იმპლემენტაციებმა ასევე აჩვენეს წარმადობის მნიშვნელოვანი გაუმჯობესება მათი პარალელურობისა და ხელახალი კონფიგურაციის გამოყენებით, რაც აჩქარებს პოლინომიურ გამრავლებას, მოდულურ არითმეტიკას და კიბერისთვის სხვა არსებით ოპერაციებს. მკვლევარებმა შეიმუშავეს ახალი აპარატურის დიზაინი და ტექნიკა ამ ოპერაციების დასაჩქარებლად [45].

შესამჩნევი მიღწევაა სწრაფი აპარატურის დიზაინის შემუშავება პოლინომიური გამრავლებისთვის NTT-ის გამოყენებით CRYSTAL-Kyber და CRYSTAL-Dilithium-ში. ამ შემთხვევებში ვიყენებთ ციფრული სიგნალის დამუშავების (DSP) მიდგომებს [46]. ეს დიზაინები ამცირებს კრიტიკული გზის შეფერხებებს და აუმჯობესებს გარემოს და შესრულებას გამოყოფილი DSP ერთეულებით.

ასევე, მეცნიერები მუშაობენ კიბერის ეფექტურობის გასაუმჯობესებლად კომპაქტური ინსტრუქციების ნაკრების გაფართოებით და გაუმჯობესებული მოდულური გამრავლების მეთოდებით [47], რაც საშუალებას მისცემს კიბერს ეფექტურად შეძლოს მუშაობა რესურსებით შეზღუდულ მოწყობილობებზე.

მიუხედავად იმისა, რომ აპარატურების ამ მიღწევებმა გაზარდა გამოყენებადობა, უსაფრთხოება რჩება მთავარ პრიორიტეტად. უახლესმა კვლევებმა გვიჩვენა დაუცველობა გვერდითი არხის თავდასხმების მიმართ, სადაც თავდამსხმელები იყენებენ გვერდითი არხის ინფორმაციას, დაშიფვრის გასაღებების ამოსაღებად. ამ საფრთხეების დასაძლევად მკვლევარებმა შემოგვთავაზეს მიდგომები, როგორიცაა რეკურსიული სწავლება და მასკირების გამოყენება უსაფრთხოების გასაძლიერებლად [48]. გარდა ამისა, ახალი კრიპტოგრაფიული შედეგები, როგორიცაა მასკირებული პოლინომიური ოპერაციები და გასაღების დერივაციის გაუმჯობესებული პროცედურები [49], შესწავლილია კიბერის უსაფრთხოების გასაძლიერებლად, რომელიც დაგვიცავს პოტენციური თავდასხმებისგან.

6. შეტევები CRYSTALS–კიბერზე

NIST-მა რეკომენდაცია გაუწია CRYSTALS-კიბერს პოსტ–კვანტური დაშიფვრისთვის. მკვლევარებმა წარმატებით გამოიყენეს გვერდითი არხის თავდასხმები, ისარგებლეს ენერგიის მოხმარების მონაცემებით და ეს გამოადგად ალგორითმის მუშაობის პროცესის გასარღვევად, დაშიფვრის გასაღების გამოსავლენად. კონკრეტულად ამ შეტევაში, CRYSTALS-კიბერის შემთხვევაში გამოიყენეს მანქანური სწავლება ენერგიის რყევების გასაანალიზებლად, რაც ახლაც მზარდი უსაფრთხოების პრობლემაა.

მიუხედავად ამისა, CRYSTALS-Kyber არ ითვლება რომ არის "გატეხილი" ან "დანგრეული". ასეთი თავდასხმების ალბათობა რეალურ სამყაროში დაბალია. თუმცა, ეს ინციდენტი ხაზს უსვამს უსაფრთხოების ისეთი პოტენციური საფრთხეების ინფორმირებულობის აუცილებლობას. უახლესი შეტევები განვითარდა და გამოწვეულია მანქანური სწავლებით. ალგორითმი დაცულია და არ არის საჭირო ზედმეტად ღელვა მის უსაფრთხოებაზე.

წინა კვლევები იყენებდა AI-ს პირველი, მეორე და მესამე რიგის მასკირებული კიბერის იმპლემენტაციების დასარღვევად, მაგრამ უფრო მაღალი დონის მასკების გატეხვა ტრადიციული მეთოდებით გატეხვა რთულია, ასევე ტრადიციული AI მეთოდებითათ. Dubrova et al. დაძლიეს ეს პრობლემა ღრმა სწავლის ახალი ტექნიკისა და შეტყობინებების ბრუნვის გამოყენებით, ბიტის გაჟონვის გაზრდის მიზნით, რაც აძლიერებს შეტევების წარმატებას [50]. მათ მეთოდი აჩვენეს კიბერის პირველი რიგის მასკირების C ვერსიაზე, გააფართოვეს იგი უფრო მაღალი დონის მასკირების შემთხვევებისთვის და გააანალიზეს ენერგიის მოხმარება კიბერის ხელახალი დაშიფვრის ფაზაში.

თავდამსხმელის შეტევა ხდება დეკაფსულაციის სტადიის შემდეგ. საზიარო გასაღების ამოღების შემდეგ, ის ხელახლა იქმნება დეკაფსულაციის პროცესში და მოწმდება ორიგინალური დაშიფრული ტექსტის არის თუ არა შეცვლილი. საიდუმლო, ან საერთო გასაღების წინამორბედი, ბიტ–ბიტებით ინახება პოლინომში ხელახალი დაშიფვრის პროცესისთვის. უფრო კონკრეტულად, 256-ბიტიანი საიდუმლო უნდა გარდაიქმნას მრავალწევრიან მოდულად $q = 3329$, რომელიც არის 256 კოეფიციენტით, სადაც i-ური კოეფიციენტი უდრის $(q-1)/2$ იმ შემთხვევაში, როდესაც i-ური ბიტი არის 1, ხოლო 0 სხვა შემთხვევაში. მიუხედავად იმისა, რომ ფუნქცია მარტივი ჩანს, შესაძლოა რთული იყოს მასკირებული ვერსიის შექმნა. პრობლემა არის ის, რომ ნაწილები, რომლებიც ერთად ქმნიან საიდუმლოს, არის ბუნებრივი მეთოდი საიდუმლოების ნაწილების წარმოებისთვის, ისევე როგორც ნაწილები, რომლებიც ერთად ემატება მრავალწევრს, არის პოლინომიალის გაზიარების ბუნებრივი გზა.

სხვა კვლევებისგან განსხვავებით, ამ შემთხვევაში AI იყენებს რეკურსიულ სწავლებას პროფილირების ფაზის დროს, არსებითად, w - რიგის მასკირებული იმპლემენტაციის სწავლება გულისხმობს M^{w-1} მოდელის Batch ნორმალიზების ფენის წონების დუბლირებას, რომელიც მომზადებულია $(w-1)$ რიგის მასკირებულ იმპლემენტაციაზე. ამის შემდეგ შრე ფართოვდება, რომ მივითოთ საწყისი ქსელის M^w. რეკურსიული სწავლება გამოიყენება იმ შემთხვევაში, როდესაც მასკირებით შრეების რაოდენობა სამზე მეტია ანუ $w > 3$. უფრო

მცირე მასკირების რიგის შემთხვევაში შესაძლებელია გამოვიყენოთ ჩვეულებრივი მანქანური სწავლება და არ მოითხოვს ახალი რეკურსიული მიდგომის გამოყენებას. ამ მეთოდში AI–ის სწავლება ხდება ქსელის გამოყენებით ჩვეულებრივი შემთხვევითი წონის განაწილებით, როდესაც $w \leq 3$.

ორი უნივერსალური მოდელი, M_0^w და M_1^w მიიღება ბაიტის მიხედვით დაჭრის და შეერთების სასწავლო კვალის გამოყენებით. ეს პროცესი აღადგენს ყველაზე ძლიერი გაჟონვის ადგილს, რომელიც არის თითოეული შეტყობინების ბაიტის პირველი და მეორე ბიტი. ესე იგი, შეტყობინების პირველ ნაწილში უფრო მეტი ინფორმაცია გაიჟონება ვიდრე ბოლო ნაწილში. გარდა ამისა, შეტყობინებების ბიტები "0" და "1" გამოიყენება როგორც ეტიკეტები და AI-ებს ასწავლიან შეტყობინების მიღებას პირდაპირ, ყოველი გამეორების დროს შემთხვევითი მასკირებების მოხსნის გარეშე.

თითოეული ბაიტის ბოლო ექვსი ბიტი გადაინაცვლებს პირველი ორი ბიტის პოზიციებზე მას შემდეგ, რაც შეტყობინება სამჯერ შემობრუნდება. ეს მეთოდი ეხმარება ბიტის მნიშვნელობების უფრო საიმედოდ ამოღებას „უფრო გაჟონვის“ ბიტების მდებარეობების გამოყენებით, რაც ზრდის შეტევის წარმატების კოეფიციენტს.

თავდასხმის ეტაპი იყენებს ციკლური როტაციის მიდგომას. ეს გამოიყენება masked_poly_frommsg()–დან გაჟონვის არაერთგვაროვანი განაწილების გამო, რაც გამოიხატება 0-დან 7-მდე ბიტებს შორის წარმატებული აღდგენის ალბათობის 9%-იანი შეუსაბამობით. მოცემული module-LWEs არის ring-LWE-ების გაფართოებები, რომელთა დაშიფრული ტექსტები შეიძლება შეიცვალოს მათი შეტყობინებების ციკლურად როტაციისთვის. თითოეული ბაიტის ბოლო 6 ბიტი საწყის 2 ბიტზე გადაბრუნებით, შეტევა აბრუნებს შეტყობინებას ნეგაციკლურად სამჯერ, 2 ბიტით. ეს საშუალებას აძლევს ბიტებს გაჟონოს მეტი ინფორმაცია ზედმეტი დროის გამოყენების გარეშე, სხვა ციკლური მიდგომებისგან განსხვავებით.

შესატყვისი დაშიფრული ტექსტის მანიპულირება საშუალებას აძლევს ადამიანს შეცვალოს შეტყობინება. პოლინომები რგოლში $\mathbb{Z}_q[X]/(X^{256}+1)$ ქმნის დაშიფრულ ტექსტს $c = (u, v)$ CRYSTALS-Kyber-ში. შეტყობინების ნეგაციკლური როტაცია შეიძლება მივიღოთ u-ს და v-ის გამრავლებით განუსაზღვრელ X-ზე, იმ პირობით, რომ c სწორად არის შექმნილი. Decode (-y) და decode (y) შეიძლება შევაფასოთ სხვადასხვა მნიშვნელობებით, ამის გამო ამ მიდგომამ შეიძლება გამოიწვიოს შეცდომები საიდუმლო გასაღების აღდგენის მცდელობებში, როდესაც გამოვიყენებთ კონკრეტული დაშიფრული ტექსტებისთვის [51-52].

გაყოფილი ორი ნაწილი შემოიფარგლება კოდით. ის ქმნის მასკას ყოველი ბიტისთვის, რომელიც არის 0xffff, თუ ბიტი იყო 1, ხოლო 0 სხვა შემთხვევაში. საჭიროების შემთხვევაში, ეს ნიღაბი გამოიყენება მრავალწევრის, პოლინომიალის წილის გასაზრდელად $(q+1)/2$-ით. 1-ის დასამუშავებლად მას ცოტა მეტი ელექტროენერგია დასჭირდება. AI არ არის საჭირო იმის დასადგენად, რომ ეს ფუნქცია გაჟონავს. ეს სიტუაცია აღინიშნა 2016 წელს, რომ ეს პატერნი ცუდი იყო. 2020 წელს კი გამოჩნდა, რომ შესაძლოა არსებობდეს ფარული კიბერის

რისკი. როგორც შესაბამისი საპასუხო ღონისძიება, მრავალი ბიტის ერთდროულად დამუშავება არის ერთ-ერთი ტექნიკა ამის შესამცირებლად.

ავტორები, Dubrova და სხვები არ ამტკიცებენ, რომ ეს არის რადიკალურად ახალი თავდასხმა. პირიქით, ისინი აძლიერებენ თავდასხმის ეფექტურობას ორი გზით: ნერვული ქსელის სწავლებით და იმის გარკვევით, თუ როგორ შეიძლება უკეთესად გამოვიყენოთ მრავალი გზა/ბილიკი გაგზავნილი დაშიფრული ტექსტის შეცვლით. ავტორებმა გამოსცადეს შემოთავაზებული შეტევა შემდეგ მოწყობილობაზე: გამოიყენეს ARM Cortex-M4 CPU, რომელსაც გააჩნია STM32F415-RGT6 მოწყობილობა, CW308 UFO დაფა და CW308T-STM32F4 სამიზნე დაფა, რომელიც მუშაობს 24 MHz-ზე, ენერგიის მოხმარება იზომება მაღალი 10-ბიტიანი სიზუსტით 24 MHz.

ნერვული ქსელების მომზადების მიზნით, გროვდება 150,000 დენის კვალი სხვადასხვა დაშიფრული ტექსტების გაშიფვრისთვის ერთი და იგივე KEM გასაღების წყვილისთვის (ცნობილი საერთო გასაღებით). რეალურ სამყაროში თუ გვინდა მსგავსი თავდასხმა, ეს უკვე უჩვეულოა, რადგან საკვანძო შეთანხმებებისთვის KEM გასაღების წყვილები დროებითია, რაც ნიშნავს, რომ ისინი იქმნება და გამოიყენება მხოლოდ ერთხელ. თუმცა, გრძელვადიანი KEM გასაღების წყვილებს აქვთ რამდენიმე მოქმედი აპლიკაცია, მათ შორის ECH, HPKE და ავტორიზაცია.

გაწვრთნა გადამწყვეტია, რადგან ერთი და იგივე ბრენდისა და მოდელის მოწყობილობებსაც კი შეუძლიათ აჩვენონ სხვადასხვა სიმძლავრის კვალი ერთი და იგივე კოდის გაშვებისას. ნერვული ქსელების ვარჯიში, სწავლება აუცილებელია. ვწრთვნით შეტევაზე „ნაწილების“ ან იმპლემენტაციების უსაფრთხოების სხვადასხვა დონეზე. ექვს ნაწილად გაყოფილი (ანუ მასკირების მეხუთე დონე) იმპლემენტაციის შეტევისთვის, ძალაუფლების კვალის მეხუთედი მოდის ექვსწილიანი განხორციელებიდან, მეხუთედი ხუთ წილიდან და ა.შ. ნაკლებად სავარაუდოა, რომ ვინმემ გამოიყენოს მოწყობილობა, რომელიც საშუალებას აძლევს შეცვალოს გაზიარებული რიცხვები.

როგორც ავტორებმა აღნიშნეს, ფაქტობრივი შეტევა იწყება იმით, რომ იდეალურ პირობებში მათ შეეძლოთ საერთო გასაღების ამოღება ორი ნაწილიანი დეკაფსულაციის ერთი სიმძლავრის კვალიდან. გასაღების ამოღების შანსი არის 0,127%. ისინი არ გვაძლევენ რიცხვით ინფორმაციას ორზე მეტ აქციაზე ერთი კვალის ნაშალიდან (shares).

გვერდითი არხის თავდასხმები უფრო წარმატებულია ერთი და იგივე დეკაფსულაციის მრავალი კვალით. ერთი და იმავე შეტყობინების კვალის დატოვების ნაცვლად, ავტორები ატრიალებენ დაშიფრულ ტექსტს. ეს ზრდის წარმატების კოეფიციენტს 78%-მდე ოთხი კვალის, ორი წილის იმპლემენტაციისთვის. ექვსი ნაწილი გაყოფის შემთხვევაში იმპლემენტაცია კვლავ ძლიერია, 0.5%. როდესაც დაშვებულია 20 კვალის, გზის ექვსწილიანი იმპლემენტაციიდან, საზიარო გასაღების 87% შეიძლება აღვადგინოთ.

2.5 K შეტყობინებები არჩეულია შემთხვევით ყოველი w-რიგის ნიღბიანი, მასკირებული განხორციელებისთვის. ვინაიდან თითოეული კვალი შეიცავს სამი 2-ბიტიანი ციკლური შეტყობინების ბრუნვას, სულ არის 10 K კვალი თითოეული შეტყობინებისთვის., თუკი არ

გამოვიყენებთ ციკლურ ბრუნვას/როტაციას. შეტყობინების აღდგენის საშუალო ალბათობა პირველი რიგის მასკირებული განხორციელებისთვის ერთი კვალით არის 0,127%. ციკლური ბრუნვები ზრდის ამ შანსს 78,866%-მდე. ალბათობა არის 0.56% მეხუთე რიგის მასკირებულ განხორციელებაზე ციკლური ბრუნვის გამოყენებით ერთი კვალის შემთხვევაში, 54.53% სამი კვალის და 87.085% ხუთი კვალის შემთხვევაში.

ტექნიკის თვალსაზრისით, ის შეიძლება გარკვეულწილად წააგავდეს სმარტ ბარათს, მაგრამ მნიშვნელოვნად განსხვავდება მაღალი დონის გაჯეტებისგან, როგორიცაა დესკტოპის კომპიუტერები, სერვერები და მობილური ტელეფონები. უბრალოდ ინტეგრირებული 1 გიგაჰერციანი პროცესორების პირობებშიც კი, გვერდითი არხის მარტივი ანალიზის თავდასხმები გაცილებით რთულია, მათ სჭირდებათ ათიათასობით კვალი პროცესორთან ახლოს განთავსებული მაღალი დონის ოსცილოსკოპით. სერვერზე ამ ტიპის ფიზიკური წვდომა გვთავაზობს ბევრად უკეთეს შეტევის ვექტორებს; ამისთვის მხოლოდ საჭიროა დავაკავშიროთ ოსცილოსკოპი მეხსიერებას (memory bus).

ელექტროენერგიის არხზე თავდასხმები ზოგადად განიხილება, როგორც არარიალიზებადი, გარდა უკიდურესად მგრძნობიარე აპლიკაციებისა. თუმცა, დახშობამ შეიძლება ზოგჯერ გამოიწვიოს ძალზე ძლიერი გვერდითი არხის თავდასხმა, რომელიც გადაიქცევა დისტანციური დროის შეტევად (distant timing attack). მტკიცედ რომ ვთქვათ, ეს შეტევა ახლოსაც არ არის იმასთან, რაც ხდება.

გარდა ამისა, ეს შეტევა არ არის ძალიან ძლიერი ან მოულოდნელი, თუნდაც გარკვეული მგრძნობიარე აპლიკაციებისთვის, როგორიცაა ჭკვიანი ბარათები. პრაქტიკაში, არ აქვს მნიშვნელობა, შენიღბული იმპლემენტაცია გაამჟღავნებს თუ არა თავის საიდუმლოებას - ის ყოველთვის აკეთებს. საკითხავია, რამდენად რთულია რეალურ ცხოვრებაში ამ შეტევის შესრულება და უღირს თუ არა თავდამსხმელს მასზე დროის დაკარგვა. მსგავსი სტატიები ეხმარება მწარმოებლებს განსაზღვრონ რამდენი საპასუხო ღონისძიება გამოიყენონ, რათა მსგავსი სტილის თავდასხმების რეალურ გარემოში შესრულება რთული და უზომოდ ძვირი იყოს.

7. საწინააღმდეგო ზომები

არსებული თავდასხმების უმრავლესობისგან საუკეთესო დაცვა არის აპლიკაციის საიდუმლო გასაღების ხანგრძლივობის შემცირება. თავდასხმა უფრო რთული იქნება, რაც უფრო ნაკლები იქნება საიდუმლო გასაღები საჯარო. თავდამსხმელს შეუძლია გამოიყენოს შეტყობინების აღდგენის შეტევა მხოლოდ იმ შემთხვევაში, თუ საიდუმლო გასაღები გამოიყენება მხოლოდ ერთხელ. თუმცა, ამან შეიძლება გამოიწვიოს სხვა პრობლემებიც. მაგალითად, შეიძლება საჭირო გახდეს საიდუმლო გასაღებების დიდი რაოდენობის შექმნა, თუ არა საიდუმლო გასაღებების გამოყენება აღმოიფხვრება.

თუკი შეუძლებელია დეკაფსულაციის პროცედურის განმეორებით ჩატარება, მოცემული შეტევა წარმატებით ვერ შესრულდება. შეზღუდვა, რამდენჯერ შეიძლება მოხდეს ერთი და იგივე შიფრული ტექსტის დეკაფსულაცია იმავე საიდუმლო გასაღებით, დაგვეხმარება ამის

მიღწევაში. შეიძლება დაგჭირდეს რამდენიმე გამეორების დაშვება, რათა მიიღოთ შემთხვევითი კომუნიკაციის შეცდომები (andom communication errors).

ალტერნატივად შეიძლება გამოვიყენოთ უფრო ძლიერი დაცვის სისტემები სიმძლავრის ანალიზის თავდასხმებისგან, როგორიცაა: დუბლირება საათის რანდომიზაციის მიდგომა (duplication with clock randomization approach) [53]. მთავარი და მოჩვენებითი კრიპტოგრაფიული ბირთვი არის ორი იდენტური ბირთვი, რომლებიც ქმნის დაცულ იმპლემენტაციას. მიუხედავად იმისა, რომ ორი ბირთვი იყენებს ორ განსხვავებულ საიდუმლო და საჯარო გასაღების წყვილს მათი შესაბამისი ამოცანებისთვის, მათ აკონტროლებს ორი განსხვავებული რანდომიზირებული საათი და იღებენ იდენტურ შეყვანის მონაცემებს. ასეთ ტექნიკას აქვს შემდეგი უპირატესობები თუკი მასკირებას შევადარებთ: ნულოვანი საათის ციკლის ზედმეტად, იმუნიტეტი ხარვეზების მიმართ, უნივერსალური დაფარვა და უფრო მაღალი გამძლეობა განმეორებითი თავდასხმების მიმართ.

8. დასკვნა

შემოთავაზებული გასაღების ინკაფსულაციის სისტემა, CRYSTALS-Kyber, მზარდი სირთულეების წინაშე დგას სხვადასხვა გვერდითი არხის თავდასხმების გამო. მიმდინარე კვლევები ავლენს სისუსტეებს ძლიერი უსაფრთხოების შემთხვევაშიც კი, რაც მოითხოვს მუდმივად დაცვის სისტემების გაუმჯობესებას. მასკირება და არევა (shuffling) არის ორი საწინააღმდეგო ღონისძიება, რომლებიც აუცილებელია კრიპტოგრაფიული სისტემების გასაძლიერებლად. როდესაც ჩვენ ვუახლოვდებით პოსტ–კვანტურ ეპოქას, აუცილებელია შევაფასოთ ალფორითმები, როგორც მათემატიკური სიძლიერისთვის, ასევე გვერდითი არხის თავდასხმებისადმი მდგრადობისთვის.

დაშიფვრის ახალი მეთოდების სრულად გარღვევის ნაცვლად, AI-ს შეუძლია დაეხმაროს ხმაურიანი მონაცემების მართვაში და ელექტროენერგიის გვერდითი არხის თავდასხმა და პირდაპირი კრიპტოგრაფიის დარღვევა ძალიან განსხვავდება ერთმანეთისგან. მიუხედავად იმისა, რომ ფაქტობრივი შეტევები იყენებს რამდენიმე კვალს, ღრმა სწავლას შეუძლია ივარჯიშოს ძალიან ხმაურიან კვალზე. ამ დისკუსიის საინტერესო ნაწილი ის არის, რომ პირდაპირი, ხელმისაწვდომი და ეფექტური თავდაცვითი საშუალებების ნაკლებობა გვაქვს ძლიერი, გვერდითი არხის თავდასხმების შესაჩერებლად.

9. დადასტურება/აღიარება

კვლევა [NFR-22-14060] განხორციელდა შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის ფინანსური მხარდაჭერით.

ბიბლიოგრაფია

1. Buchmann, J., Dahmen, E., Szydlo, M. (2009). Hash-based Digital Signature Schemes. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_3
2. Chen, Lily, et al. Report on post-quantum cryptography. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2016.
3. Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41, no. 2 (1999): 303-332.
4. Iavich, Maksim, et al. "ADVANTAGES AND CHALLENGES OF QRNG INTEGRATION INTO MERKLE." Scientific and practical cyber security journal (2020).
5. Gagnidze, Avtandil, Maksim Iavich, and Giorgi Iashvili. "Novel version of merkle cryptosystem." Bulletin of the Georgian National Academy of Sciences (2017).
6. Iavich, M., Kuchukhidze, T., & Bocu, R. (2023). A Post-Quantum Digital Signature Using Verkle Trees and Lattices. Symmetry, 15(12), 2165.
7. Alagic, Gorjan, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger et al. "Status report on the third round of the NIST post-quantum cryptography standardization process." US Department of Commerce, NIST (2022).
8. Announcing the commercial national security algorithm suite 2.0. National Security Agency, U.S Department of Defense https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
9. Avanzi, Roberto, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "CRYSTALS-Kyber algorithm specifications and supporting documentation." NIST PQC Round 2, no. 4 (2019): 1-43.
10. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Annual international cryptology conference. pp. 388–397. Springer (1999)
11. Wu, L., Perin, G., Picek, S. (2022). On the Evaluation of Deep Learning-Based Side-Channel Analysis. In: Balasch, J., O'Flynn, C. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2022. Lecture Notes in Computer Science, vol 13211. Springer, Cham. https://doi.org/10.1007/978-3-030-99766-3_3
12. Wang, R., Ngo, K., Dubrova, E.: A message recovery attack on LWE/LWR-based PKE/KEMs using amplitude-modulated EM emanations. In: Proc. of 25th Annual Int. Conf. on Information Security and Cryptology (2022), https://eprint.iacr. org/2022/852
13. Fritzmann, T., Van Beirendonck, M., Basu Roy, D., Karl, P., Schamberger, T., Verbauwhede, I., & Sigl, G. (2021). Masked accelerators and instruction set extensions for post-quantum cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022(1), 414-460.
14. Gigerl, B., Primas, R., & Mangard, S. (2023, May). Formal verification of arithmetic masking in hardware and software. In International Conference on Applied Cryptography and Network Security (pp. 3-32). Cham: Springer Nature Switzerland.
15. Coron, J. S., Gérard, F., Montoya, S., & Zeitoun, R. (2021). High-order polynomial comparison and masking lattice-based encryption. Cryptology ePrint Archive.
16. Ngo, K., Dubrova, E., Johansson, T.: Breaking masked and shuffled CCA secure Saber KEM by power analysis. In: Proc. of the 5th Workshop on Attacks and Solutions in Hardware Security. pp. 51–61 (2021)
17. Kairouz, P., McMahan, B., Song, S., Thakkar, O., Thakurta, A., & Xu, Z. (2021, July). Practical and private (deep) learning without sampling or shuffling. In International Conference on Machine Learning (pp. 5213-5225). PMLR.

18. Nguyen, T. T., Trahay, F., Domke, J., Drozd, A., Vatai, E., Liao, J., ... & Gerofi, B. (2022, May). Why globally re-shuffle? Revisiting data shuffling in large scale deep learning. In 2022 IEEE International Parallel and Distributed Processing Symposium (IPDPS) (pp. 1085-1096). IEEE.
19. Brisfors, M., Moraitis, M., & Dubrova, E. (2022). Side-channel attack countermeasures based on clock randomization have a fundamental flaw. Cryptology ePrint Archive.
20. Jayasinghe, D., Udugama, B., & Parameswaran, S. (2023, January). FPGA Based Countermeasures Against Side channel Attacks on Block Ciphers. In Proceedings of the 28th Asia and South Pacific Design Automation Conference (pp. 365-371).
21. Coron, Jean-Sébastien, and Ilya Kizhvatov. "An efficient method for random delay generation in embedded software." In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 156-170. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.
22. Leplus, G., Savry, O., & Bossuet, L. (2022, June). Insertion of random delay with context-aware dummy instructions generator in a RISC-V processor. In 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 81-84). IEEE.
23. Xagawa, K., Ito, A., Ueno, R., Takahashi, J., & Homma, N. (2021). Fault-injection attacks against NIST's post-quantum cryptography round 3 KEM candidates. In Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part II 27 (pp. 33-61). Springer International Publishing.
24. Maghrebi, H., Servant, V., & Bringer, J. (2016). There is wisdom in harnessing the strengths of your enemy: Customized encoding to thwart side-channel attacks. In Fast Software Encryption: 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers 23 (pp. 223-243). Springer Berlin Heidelberg.
25. Belleville, N., Couroussé, D., Heydemann, K., & Charles, H. P. (2018). Automated software protection for the masses against side-channel attacks. ACM Transactions on Architecture and Code Optimization (TACO), 15(4), 1-27.
26. Kreuzer, K. (2023). Verification of Correctness and Security Properties for CRYSTALS-KYBER. Cryptology ePrint Archive.
27. Wang, Z., Meng, F. H., Park, Y., Eshraghian, J. K., & Lu, W. D. (2023). Side-channel attack analysis on in-memory computing architectures. IEEE Transactions on Emerging Topics in Computing.
28. Moraitis, M., Ji, Y., Brisfors, M., Dubrova, E., & Lindskog, N. (2023). Securing CRYSTALS-Kyber in FPGA Using Duplication and Clock Randomization. IEEE Design & Test.
29. Jeon, H., Xie, J., Jeon, Y., Jung, K. J., Gupta, A., Chang, W., & Chung, D. (2023). Statistical power analysis for designing bulk, single-cell, and spatial transcriptomics experiments: review, tutorial, and perspectives. Biomolecules, 13(2), 221.
30. Zulberti, L., Di Matteo, S., Nannipieri, P., Saponara, S., & Fanucci, L. (2022). A script-based cycle-true verification framework to speed-up hardware and software co-design: Performance evaluation on ecc accelerator use-case. Electronics, 11(22), 3704.
31. Köpf, B., & Dürmuth, M. (2009, July). A provably secure and efficient countermeasure against timing attacks. In 2009 22nd IEEE Computer Security Foundations Symposium (pp. 324-335). IEEE.
32. He, J., Guo, X., Tehranipoor, M. M., Vassilev, A., & Jin, Y. (2022). EM Side Channels in Hardware Security: Attacks and Defenses. IEEE Des. Test, 39(2), 100-111.
33. Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography. IEEE Access.
34. Hofheinz, Dennis, Kathrin Hövelmanns, and Eike Kiltz. "A modular analysis of the Fujisaki-Okamoto transformation." In Theory of Cryptography Conference, pp. 341-371. Cham: Springer International Publishing, 2017.

35. Kocher, Paul C. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems." In Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16, pp. 104-113. Springer Berlin Heidelberg, 1996.
36. Ngo, Kalle, Elena Dubrova, Qian Guo, and Thomas Johansson. "A side-channel attack on a masked IND-CCA secure saber KEM implementation." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 676-707.
37. Bhasin, Shivam, Jan-Pieter D'Anvers, Daniel Heinz, Thomas Pöppelmann, and Michiel Van Beirendonck. "Attacking and defending masked polynomial comparison for lattice-based cryptography." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 334-359.
38. Guo, Q., Nabokov, D., Nilsson, A., & Johansson, T. (2023, December). Sca-ldpc: A code-based framework for key-recovery side-channel attacks on post-quantum encryption schemes. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 203-236). Singapore: Springer Nature Singapore.
39. Xu, Zhuang, Owen Pemberton, Sujoy Sinha Roy, David Oswald, Wang Yao, and Zhiming Zheng. "Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of kyber." IEEE Transactions on Computers 71, no. 9 (2021): 2163-2176.
40. Ravi, Prasanna, Shivam Bhasin, Sujoy Sinha Roy, and Anupam Chattopadhyay. "Drop by Drop you break the rock-Exploiting generic vulnerabilities in Lattice-based PKE/KEMs using EM-based Physical Attacks." IACR Cryptol. ePrint Arch. 2020 (2020): 549.
41. Beirendonck, Michiel Van, Jan-Pieter D'anvers, Angshuman Karmakar, Josep Balasch, and Ingrid Verbauwhede. "A side-channel-resistant implementation of SABER." ACM Journal on Emerging Technologies in Computing Systems (JETC) 17, no. 2 (2021): 1-26.
42. Ngo, Kalle, Elena Dubrova, Qian Guo, and Thomas Johansson. "A side-channel attack on a masked IND-CCA secure saber KEM implementation." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 676-707.
43. Bisheh-Niasar, M., Azarderakhsh, R., & Mozaffari-Kermani, M. (2021). Instruction-set accelerated implementation of CRYSTALS-Kyber. IEEE Transactions on Circuits and Systems I: Regular Papers, 68(11), 4648-4659.
44. Di Matteo, S., Sarno, I., & Saponara, S. (2024). CRYPHTOR: A Memory-Unified NTT-Based Hardware Accelerator for Post-Quantum CRYSTALS Algorithms. IEEE Access, 12, 25501-25511.
45. Nguyen, T. H., Kieu-Do-Nguyen, B., Pham, C. K., & Hoang, T. T. (2024). High-speed NTT Accelerator for CRYSTAL-Kyber and CRYSTAL-Dilithium. IEEE Access.
46. Wang, H., Zhou, J., Xing, Z., Feng, Q., Zhang, K., Zheng, K., ... & Li, Z. (2023). Fast-convergence digital signal processing for coherent PON using digital SCM. Journal of Lightwave Technology, 41(14), 4635-4643.
47. Li, L., Qin, G., Yu, Y., & Wang, W. (2023). Compact Instruction Set Extensions for Kyber. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.
48. Zhao, Y., Pan, S., Ma, H., Gao, Y., Song, X., He, J., & Jin, Y. (2023). Side channel security oriented evaluation and protection on hardware implementations of kyber. IEEE Transactions on Circuits and Systems I: Regular Papers.
49. Kundu, S., Karmakar, A., & Verbauwhede, I. (2023, December). On the Masking-Friendly Designs for Post-quantum Cryptography. In International Conference on Security, Privacy, and Applied Cryptography Engineering (pp. 162-184). Cham: Springer Nature Switzerland.
50. Dubrova, Elena, Kalle Ngo, Joel Gärtner, and Ruize Wang. "Breaking a fifth-order masked implementation of crystals-kyber by copy-paste." In Proceedings of the 10th ACM Asia Public-Key Cryptography Workshop, pp. 10-20. 2023.

51. Azouaoui, Melissa, Yulia Kuzovkova, Tobias Schneider, and Christine van Vredendaal. "Post-quantum authenticated encryption against chosen-ciphertext side-channel attacks." Cryptology ePrint Archive (2022).
52. Backlund, Linus, Kalle Ngo, Joel Gärtner, and Elena Dubrova. "Secret Key Recovery Attack on Masked and Shuffled Implementations of CRYSTALS-Kyber and Saber." In International Conference on Applied Cryptography and Network Security, pp. 159-177. Cham: Springer Nature Switzerland, 2023.
53. Nikova, Svetla, Christian Rechberger, and Vincent Rijmen. "Threshold implementations against side-channel attacks and glitches." In International conference on information and communications security, pp. 529-545. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.