Kafes-Tabanlı Anahtar Değişim/Paketleme Protokollerinde Kullanılan Uzlaşma Yöntemlerine Ait Bileşenlerin Analizi

On the Analysis of Components of Reconciliation Mechanisms in Lattice-Based Key Exchange/Encapsulation Protocols

Sedat AKLEYLEK
Ondokuz Mayıs Üniversitesi, Bilgisayar Mühendisliği Bölümü, Samsun, Türkiye
sedat.akleylek@bil.omu.edu.tr
0000-0001-7005-6489

Kübra SEYHAN
Ondokuz Mayıs Üniversitesi, Bilgisayar Mühendisliği Bölümü, Samsun, Türkiye
kubra.seyhan@bil.omu.edu.tr
0000-0002-0902-1903

Öz

Kafes-tabanlı Diffie-Hellman benzeri anahtar değişim/paketleme protokollerinde kullanılan zor problemlerin yapısı gereği ortak paylaşılan anahtarın elde edilmesinde ara işlem adımlarına ihtiyaç duyulur. Uzlaşma yapıları olarak isimlendirilen bu adımların farklılaşması ile kuantum sonrası kriptografi için alternatif sistemler önerilebilecektir. Bu çalışmada, RLWE problemi tabanlı Ding17, Peikert14, Saarinen17 ile MLWE problemi tabanlı Hamburg17 ve Bi-GISIS problemi tabanlı Jing18 anahtar değişim/paketleme protokolleri içerdikleri problemlere, kullanılan cebirsel yapılara ve protokollerin işleyiş aşamalarına göre farklılaşan uzlaşma yöntemleri açısından karşılaştırılmıştır. Yapılan bu karşılaştırma sonucu yuvarlama işlemi ve ek bilgi hesabı içeren ve içermeyen, farklı $\mathbb{Z}_q$ parçalanışlarına sahip bir veya daha fazla uzlaşma fonksiyonu kullanan protokollerin içermesi gereken işleyiş adımları tespit edilmiştir. Elde edilen bilgiler ile yeni bir yaklaşımın içerebileceği temel yapı açıklanarak açık problemlere çözüm önerisi sunabilen gelecek çalışmalara yer verilmiştir.

Anahtar Sözcükler: *kuantum sonrası kriptografi, RLWE, MLWE, Bi-GISIS, anahtar değişim/paketleme, uzlaşma.*

Gönderme ve kabul tarihi: 22.10.2019 - 26.12.2019
Makale türü: Araştırma

Abstract

Lattice-based Diffie-Hellman like key exchange/encapsulation mechanisms require intermediate processing steps to obtain the shared secret key. These steps, called reconciliation methods, are due to the structure of the hard lattice problems. By using the variations of these steps, alternative systems for post-quantum cryptography can be proposed. In this paper, RLWE based Ding17, Peikert14, and Saarinen17 protocols, MLWE based Hamburg17 protocol, and Bi-GISIS based Jing18 protocol are compared. This comparison is made to determine the differentiated reconciliation steps according to the hard lattice problems, algebraic structures and stages of protocol operations. As a result of this comparison, some different approaches are observed in terms of reconciliation and rounding functions, the calculation of additional information, and the partitions of $\mathbb{Z}_q$. We also explain the main structure of new ideas that can be used to build reconciliation methods to solve open problems.

Keywords: *post-quantum cryptography, RLWE, MLWE, Bi-GISIS key exchange/encapsulation, reconciliation.*

1. Giriş

Anahtar değişim protokolleri, güvenli iletişimin sağlanmasında şifreleme sistemlerinde kullanılacak olan anahtarların üretilmesi fikriyle ortaya çıkmıştır. İlk olarak 1976 yılında Diffie-Hellman (DH) [1] tarafından önerilen anahtar değişim (key exchange -

KE) protokolü, güvenliğini ayrık logaritma probleminin zorluk varsayımından almaktadır. Günümüzde kullanılan hesaplama sistemlerinin bu problemi çözebilecek gücünün olmaması, DH anahtar değişim protokolünün SSL, SSH, IPSec gibi birçok protokolde güvenli iletişimin sağlanmasında aktif olarak kullanılmasına olanak sağlamıştır. Ancak Shor tarafından 1994 yılında önerilen bir algoritma [2] ayrık logaritma ve çarpanlara ayırma problemlerine polinom zamanda çözüm önerisi sunmuştur. Bu gelişme ile birlikte 1997 yılında ilk 2-kübitlik kuantum bilgisayarın üretilmesi ve beraberinde 2001 yılında 15 sayısının 5-kübitlik kuantum bilgisayar ile çarpanlarına ayrılması, büyük ölçekli kuantum bilgisayarlar varlığında ayrık logaritma ve çarpanlara ayırma problemlerinin zorluk varsayımlarına dayanan sistemlerin güvensiz hale geleceğini göstermiştir [3]. Güvensiz hale gelecek sistemlerin yerine kuantum bilgisayarlar sonrası kriptografi için alternatif güvenilir sistemlerin belirlenmesi amacıyla 2016 yılında Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology - NIST) bir standartlaşma süreci başlatmıştır [4]. Bu süreç sonunda elde edilecek olan açık anahtarlı kripto sistem veya kripto sistemlerin hem günümüz hesaplama sistemlerine hem de kuantum bilgisayarlara karşı dirençli olması hedeflenmektedir. Sayılar teorisinde bulunarak günümüz kripto sistemlerin temelini oluşturan çarpanlara ayırma ve ayrık logaritma problemlerinin yerini alarak kuantum bilgisayarlar sonrası güvenilir sistemlerin oluşturulmasında kullanılan bazı zor problemler vardır. Bu problemlerden kafes tabanlı kriptografide yer alan en kısa vektör problemi (shortest vector problem - SVP), en yakın vektör problemi (closest vector problem - CVP), hatalar ile öğrenme problemi (learning with errors - LWE) ve bu problemlere alternatif olarak önerilen zor problemler temel alınarak kuantum dirençli şifreleme ve imzalama sistemlerinin yanı sıra KE protokolleri de oluşturulabilmektedir [5]. Kuantum bilgisayarlar sonrası kafes tabanlı DH benzeri KE protokolleri için önerilen genel yaklaşım Şekil-1'de açıklanmıştır [6].

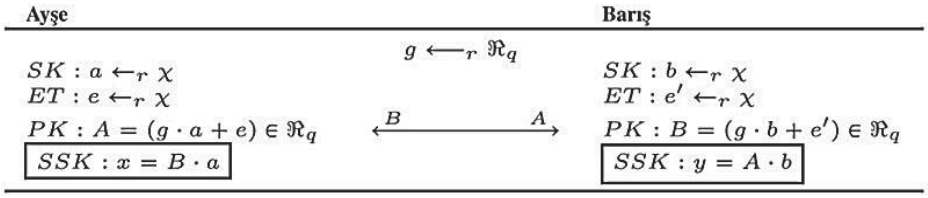
DH benzeri kafes tabanlı KE protokollerinde kullanılan zor problemlerin yapısı gereği taraflar arasında uzlaşma problemi ortaya çıkmaktadır. Şekil-1'de hata terimi (error term - ET) olarak yer alan e ve e' protokol için belirlenen olasılık dağılımından rastgele seçilerek taraflar arasında gizli anahtar (secret key - SK) olarak dağıtılmamaktadır. Protokolde yer alan $A = (g \cdot a + e)$ ve $B = (g \cdot b + e')$ açık anahtarları (public key - SK) için hesaplanan x ve y ortak paylaşımlı gizli anahtarlar (SSK);

$$x = B \cdot a = (g \cdot b + e') \cdot a = g \cdot b \cdot a + e' \cdot a$$
$$y = A \cdot b = (g \cdot a + e) \cdot b = g \cdot b \cdot a + e \cdot b$$

eşitlikleri ile ifade edilir. x'de bulunan $e' \cdot a$ ve y'de de bulunan $e \cdot b$ terimleri nedeniyle eşit SSK değerlerinin elde edilememesi uzlaşma problemi olarak adlandırılmaktadır. Bu durum kafes tabanlı zor problemleri temel alan şifreleme sistemlerinde (key encapsulation mechanism - KEM) şifre çözme aşamasında başarısızlık riski oluşturabileceği gibi KE protokollerinde tarafların verimli bir şekilde uzlaşmasını zorlaştırır. Bu sistemlerde şifre çözme ve uzlaşma aşamalarında başarısızlık oluşması riskine ara işlem adımlarının eklenmesi ile çözüm bulunur [7]. Şekil-1'de dikdörtgen içerisine alınarak vurgulanan SSK terimlerinde oluşacak uzlaşma probleminin ortadan kaldırılmasında temel olarak anahtar bileşene ait ek bilginin gönderilmesi yaklaşımını içeren ve içermeyen protokoller bulunmaktadır.

1.1. Motivasyon ve Katkı

Günümüzde güvenli haberleşmenin sağlanmasında birçok protokolde kullanılan KE/KEM protokollerinin kuantum bilgisayarlar varlığında etkisiz hale gelecek olması ihtimali DH benzeri KE ve KEM protokollerinin kuantum bilgisayarlar sonrası sistemlere uyarlanması gerekliliğini ortaya koymuştur. Bu gereklilik temel alınarak açık problem [8] olarak ifade edilen yeni uzlaşma yöntemlerinin önerilmesine bağlı olarak farklı protokollerin oluşturulması amacıyla bu çalışmada, ana işleyiş adımlarında farklılaşmalar bulunan uzlaşma yapıları ele alınmıştır. Benzer yaklaşımla gerçekleştirilen [9] nolu çalışmada ele alınan zor problemin ve ek bilgi gönderme yaklaşımının farklılaşması durumunda uzlaşma yapılarında meydana gelebilecek benzerliklerin ve farklılıkların belirlenmesi amacıyla [6], [10] ve [11] nolu çalışmalarda yer alan protokollere ek olarak [12] ve [13] nolu çalışmalarda yer alan protokoller benzer yaklaşımla özetlenerek bu protokollerde yer alan uzlaşma yöntemleri karşılaştırılmıştır. Bu karşılaştırmada [7] ve [9] nolu çalışmalarda



Şekil-1: RLWE Tabanlı DH Benzeri Anahtar Değişimin Genel Yapısı

bulunan hata dağılımı, ek bilgi gönderimi, yuvarlama, $\mathbb{Z}_q$ parçalanışı ve uzlaşma şartları yaklaşımlarına ek olarak seçilen protokollerde kullanılan fonksiyonlar ve örnek dağılımları açıklanarak zorluk varsayımına bağlı olarak değişen özellikler detaylandırılmıştır. Elde edilen bilgiler dahilinde yeni bir yaklaşımın temel fikri açıklanmıştır.

1.2. Organizasyon

Bu çalışmada, Bölüm 2'de Ding17, Peikert14, Saarinen17, Hamburg17 ve Jing18 KE/KEM protokollerinin işleyiş adımları benzer yaklaşımla özetlenerek bu protokollerde kullanılan uzlaşma yöntemlerine ait temel adımlar ve bu adımların içerdiği bileşenler açıklanmıştır. Ayrıca protokollerde farklılaşmalara neden olan fonksiyonlar detaylandırılarak uzlaşmanın gerçekleşebilmesi için gerekli şartlar ifade edilmiştir. Bölüm 3'te bu çalışmada ele alınan KE/KEM protokollerine ait belirleyici özellikler ve uzlaşma yöntemlerine ait bileşenler karşılaştırılmıştır. Son olarak Bölüm 4'te uzlaşma yöntemlerine dair literatürde yer alan açık problemler dâhilinde gelecekte yapılması planlanan çalışmalara ait genel fikir açıklanmıştır.

2. Kafes Tabanlı Anahtar Değişim/Paketleme Protokolleri

Bu bölümde kafes tabanlı KE/KEM protokollerinde kullanılan genel işleyiş adımları özetlenerek önerilen uzlaşma yöntemleri ve bu yöntemlere ait bileşenler açıklanmıştır.

Bu çalışmada kullanılan semboller ve anlamları şu şekildedir;

q: mod değeri, $\mathbb{Z}_q$: $\{0, \cdots, q-1\}$ ile ifade edilen $mod\ q$'da bulunan tam sayılar, $\mathfrak{R} = \mathbb{Z}[x](x^n + 1)$: Katsayıları tam sayı olan polinomlar halkası, $\mathfrak{R}_q = \mathbb{Z}_q[x](x^n + 1)$: Katsayıları $mod\ q$'da tam sayılar olan polinomlar halkası, χ: $\mathfrak{R}$ üzerinde tanımlı ayrık Gauss dağılımı, d: Modül cebirsel yapısının boyutu (rankı), $M \subseteq \mathfrak{R}^d$: $\forall\, m_i \in \mathfrak{R}$ için $m = (m_0, \cdots, m_{d-1}) \in M$ ile ifade edilen d-boyutlu halka elemanlarından oluşan modül cebirsel yapısı, ϕ : $\mathfrak{R}^d$ üzerinde tanımlı ayrık Gauss dağılımı, $A \in \mathfrak{R}_q^{mxm}$: $\forall\, a_i \in \mathfrak{R}_q$ olan m satır ve m sütundan oluşan matris, $D_{\mathfrak{R}^m,\sigma}$: $\mathfrak{R}^m$'de tanımlı standart sapması σ olan ayrık Gauss dağılımı, x^T: x vektörünün transpozu, $x \longleftarrow_r U[0,\ q-1]$: x, $\{0, \cdots, q-1\}$ aralığında bulunan değerlerden rastgele seçilir, p: Yuvarlama parametresi, $\lfloor x \rceil$: x'e eşit veya daha küçük en büyük tam sayı, $x \longleftarrow_r \chi$: x, χ hata dağılımından rastgele seçilir, $i = [n]$: $\{1, \cdots, n\}$, $|x|$: x'in mutlak değeri, $\|x\|_\infty = \max |x_i|$: $x \in \mathbb{R}^n$ için sonsuz norm, $\lfloor x \rceil$: x'e en yakın tam sayı, ψ_{16}^n: Binom dağılımı, , NTT: Sayı teorik dönüşümü (number theoretic transform), NTT^{-1}: Sayı teorik dönüşümünün tersi, ϑ_{σ^2}; ortalaması 0, varyansı σ^2 olan hata dağılımı, $\deg(P)$: $N = P(x)$ polinomunun derecesi, χ_{σ^2}: Modüller üzerinde tanımlı ayrık Gauss dağılımı, $\mathcal{R} = \mathbb{Z}/N\mathbb{Z}$: N sözde Mersenne asallarında tanımlı tam sayı polinomlar halkası, $D_{\mathfrak{R}^m,\sigma}$: $\mathfrak{R}^m$'de tanımlı standart sapması σ olan ayrık Gauss dağılımı.

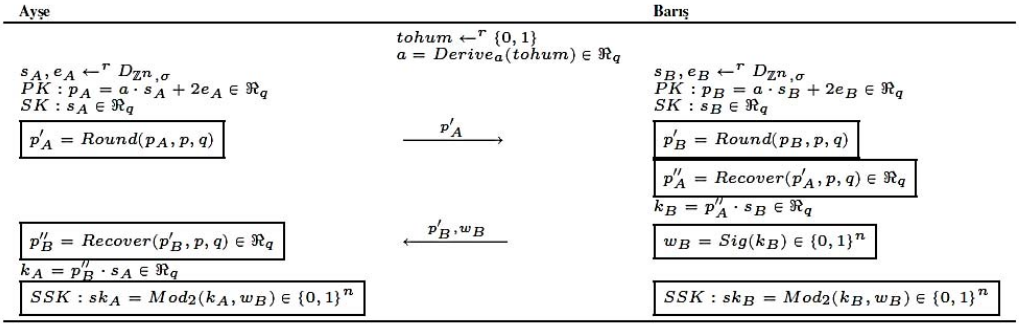
Kuantum bilgisayarlar sonrası kriptografi için önerilen KE\KEM protokolleri kafes tabanlı zor problemlerin zorluk varsayımı temel alınarak oluşturulmaktadır. Bu çalışmada ele alınan;

- Ding17, Peikert14, Saarinen17 protokolleri RLWE problemi,
- Hamburg17 protokolü MLWE problemi,
- Jing18 protokolü Bi-GISIS problemi

temel alınarak oluşturulmuştur. Bu protokollerin daha kolay anlaşılabilmesi için bahsedilen zor problemler şu şekilde açıklanabilir:

2010 yılında Lyubashevsky, Peikert ve Regev tarafından halka cebirsel yapısı temel alınarak oluşturulan hatalar ile öğrenme problemi tanımlanmıştır [14].

Tanım 1. Halkalar Üzerinde Tanımlı Hatalar ile Öğrenme Problemi – RLWE: $s \in \mathfrak{R}_q$ gizli değeri için $a \in \mathfrak{R}_q$ düzgün rastgele iken e hata teriminin χ



Şekil-2: Ding17 RLWE Tabanlı Anahtar Değişim Protokolü

$$(a, b = s \cdot a + e \; mod \; q) \in \Re_q x \Re_q$$

hata dağılımından seçildiği durumda RLWE dağılımı; eşitliği ile ifade edilir.

2013 yılında Brakerski ve arkadaşları modüller üzerinde tanımlı hatalar ile öğrenme problemini tanımlamıştır [15].

Tanım 2. Modüller Üzerinde Tanımlı Hatalar ile Öğrenme Problemi – MLWE: n boyutlu $\Re$ halkasında $M \subseteq \Re^d$ modülü tanımlansın. $s \in \Re_q^d$ gizli değeri için $a \in \Re_q^d$ düzgün rastgele seçilen bir değer iken e hata teriminin ϕ hata dağılımından seçildiği durumda MLWE dağılımı;

$$(a, b = s \cdot a + e \; mod \; q) \in \Re_q^d x \Re_q$$

eşitliği ile ifade edilir.

2018 yılında ise Jing ve arkadaşları temel zor problemlerden farklı olarak iki yönlü genelleştirilmiş homojen olmayan kısa tam sayı çözüm problemini tanımlamıştır [13].

Tanım 3. İki Yönlü Genelleştirilmiş Homojen Olmayan Kısa Tam Sayı Çözüm Problemi - Bi-GISIS: Rankı m olan $A \in \Re_q^{mxm}$ rastgele matrisi ve $s_1, s_2, e_1, e_2 \longleftarrow_r D_{\Re^m,\sigma}$ terimleri için $x_1 = As_1 + e_1 \; mod \; q$ ve $x_2^T = s_2^T A + e_2^T \; mod \; q$ vektörleri verildiğinde s_1, s_2^T gizli değerlerini bulma problemidir.

RLWE, MLWE ve Bi-GISIS problemlerini polinom zamanda kuantum bilgisayarlarda çözebilen algoritmalar henüz bilinmemektedir. Bu özellik bu problemler temel alınarak oluşturulan KE\KEM protokollerinde güvenlik kanıtı olarak sunulmaktadır. Bu problemlerin zorluk varsayımları temel alınarak oluşturulmuş güvenilir olduğu düşünülen bazı protokoller ve bu protokollerin içerdiği uzlaşma yöntemleri alt bölümlerde özetlenmiştir.

2.1. Ding17 RLWE Tabanlı Anahtar Değişim Protokolü

Ding ve arkadaşları tarafından 2017 yılında NIST'in standartlaşma süreci için önerilen protokolde yer alan uzlaşma yöntemine ait bileşenlerin açıklanabilmesi amacıyla, kullanılan KE protokolü Şekil-2'de özetlenmiştir [10].

Ding17 protokolünde RLWE dağılımından örnekler türetilmesi için örnekleme $Derive_a()$ fonksiyonu kullanılırken Ayşe'nin elde ettiği sk_A ve Barış'ın elde ettiği sk_B ortak paylaşılan gizli anahtar değerlerinin eşitliği yuvarlama $Round()$, eğilimi kaldırma $Remove\_Bias()$, kurtarma $Recover()$, ek bilgi $Sig()$ ve uzlaşma $Mod_2()$ fonksiyonları ile sağlanır. Uzlaşmanın sağlanmasında $sk_A = sk_B$ kullanılan bu fonksiyonlar iletişim maliyetinin düşürülmesi, tarafsız anahtar bileşenlerinin üretilmesi anlamında faydalar da sağlamaktadır.

Ding17 protokolü, Tanım 1'de açıklanan RLWE probleminin zorluk varsayımı temel alınarak oluşturulmuştur. Bu protokolde kullanılan anahtar değerlerin üretilebilmesi için Ding17 örnekleme fonksiyonu kullanılır.

Tanım 4. Ding17 Örnekleme Fonksiyonu - $Derive_a()$: RLWE dağılımından örnekler türetilirken kullanılan açık anahtar $a \in \Re_q$'nın üretilmesinde; 128-bitlik tohum değeri, sözde rastgele sayı üretecinin başlangıç değeri iken $i \in \{1, \cdots, n\}$ ile $\mathbb{Z}_q$'dan $a_i \longleftarrow_r U[0, \; q-1]$ seçimleri ile $a \in \Re_q$ polinomunun katsayıları üretilir.

Ding17 protokolünde hata terimlerinin $(2e_i)$ etkisinin azaltılması ve taraflara ait iletişim

maliyetinin düşürülmesi gibi amaçlarla yuvarlama fonksiyonu kullanılır.

Tanım 5. Yuvarlama Fonksiyonu – $Round()$: $x \in \mathbb{Z}_q$ ve $q > p > 0$ olsun. $x' = Round(x, p, q)$ fonksiyonunda girdi değeri x'in tek ve çift olma özellikleri korunarak $x' \leftarrow \left\lfloor p \cdot \frac{x}{q} \right\rceil$ yuvarlama işlemi ile elde edilen $x' \in \{0, \cdots, p\}$ ile hata terimlerinin etkisi azaltılarak bölgesel anlamda indirgeme sağlanır. Bu işlemler belirli pozisyonlarda eğilimin oluşmasına neden olur. Bu eğilimin ortadan kaldırılması ve tarafsız anahtar bitleri elde edilmesi amacıyla $Round()$ fonksiyonu içerisinde $x' \leftarrow x' + 2$ işlemini gerçekleştiren eğilimi kaldırma fonksiyonu olan $Remove\_Bias()$ kullanılır. $q = 120833$, $p = 7551$ parametreleri için eğilimin oluştuğu pozisyonlar: $pozisyon = \{0, 455, 888, 1333, 1776, 2221, 2666, \cdots, 7106\}$ olarak ifade edilmiştir. Bu durum parametre seçim kümesine bağlı olarak eğilimin oluştuğu pozisyonların da değişeceğini açıklamaktadır.

Yuvarlama işleminin parametreler üzerinde etkisinin dengelenmesi ve değer kayıplarının önüne geçilmesi amacıyla kurtarma fonksiyonu kullanılır.

Tanım 6. Kurtarma Fonksiyonu - $Recover()$: $x' \in \mathbb{Z}_p$ ve $q > p > 0$ olsun. $x'' = Recover(x', p, q)$ fonksiyonunda girdi değeri x''in tek ve çift olma özellikleri korunarak, $x'' \leftarrow \left\lfloor q \cdot \frac{x'}{p} \right\rceil$ işlemi ile yuvarlama fonksiyonunun etkisi dengelenir.

Ding17 protokolünde uzlaşmanın sağlanabilmesi için anahtar bileşene ait ek bilginin gönderilmesinde bileşenlerin tanımlı olduğu $\mathbb{Z}_q$'nun parçalanışı ve etiketlendirilmesi işlemi ipucu fonksiyonları ile sağlanmaktadır.

Tanım 7. İpucu Fonksiyonları - σ_i: Katsayıların tanımlı olduğu $\mathbb{Z}_q = \{-\frac{q-1}{2}, \cdots, \frac{q-1}{2}\}$' nun 4 bölgeye parçalandığı bu fonksiyonda 4 bölge için $\mathbb{Z}_q \rightarrow \mathbb{Z}_2$ dönüşümü yapılarak bu bölgeler 0 ya da 1 değerleri ile etiketlendirilir.

$$\sigma_0(x) = \begin{cases} 0, & x \in \left[-\left\lfloor \frac{q}{4} \right\rfloor, \left\lfloor \frac{q}{4} \right\rfloor\right] \leftarrow içbölge1 \\ 1, & diğer\ durumlar \leftarrow dışbölge1 \end{cases}$$

$$\sigma_1(x) = \begin{cases} 0, & x \in \left[-\left\lfloor \frac{q}{4} \right\rfloor + 1, \left\lfloor \frac{q}{4} \right\rfloor + 1\right] \leftarrow içbölge2 \\ 1, & diğer\ durumlar \leftarrow dışbölge2 \end{cases}$$

Ding17 protokolünde ipucu fonksiyonları ile belirlenen bölgeler kullanılarak anahtara ait ek bilginin hesaplanması için sinyal fonksiyonu kullanılır.

Tanım 8. Sinyal Fonksiyonu - $Sig()$: Anahtar bileşenlerin ipucu fonksiyonları ile belirlenen bölgede bulunma durumlarına göre ek bilginin belirlenmesinde kullanılan fonksiyondur. $y \in \mathbb{Z}_q$ ve $b \longleftarrow_r \{0,1\}$ için $Sig(y) = \sigma_b(x)$'dir. Daha açık bir ifadeyle katsayı y için $Sig(y) = 1$ ise y dış bölgededir.

Uzlaşma fonksiyonu kullanılarak dış bölgede bulunan katsayılar ile oluşacak olası ek mod işlemleri ortadan kaldırılarak ortak paylaşılan anahtarın eşitliği için aynı en anlamsız bit her iki taraftan da çıkarılır.

Tanım 9. Uzlaşma Fonksiyonu - $Mod_2()$: $x \in \mathbb{Z}_q$ katsayısı için ek bilgi $w = Sig(x)$ olsun.

$$Mod_2(x, w) = \left(x + w \cdot \frac{q-1}{2} mod\ q\right) mod\ 2$$

eşitliği ile katsayı dış bölgede ($w = 1$) ise $\frac{q-1}{2}$ ile çarpılarak iç bölgeye taşınır. Böylece ek mod işlemleri ortadan kaldırılarak hem iletişim maliyeti üzerinde iyileşme sağlanır hem de hata üzerinde uzlaşma gerçekleştirilir.

Şekil-2'de özetlenen Ding17 KE protokolünde taraflara ait anahtar bileşenler k_A, $k_B \in \Re_q$'dır. Bu bileşenlere ait katsayılar $i \in [n]$ için $k_{Ai}, k_{Bi} \in \mathbb{Z}_q$ iken taraflar arasında uzlaşmanın sağlanması ve tarafsız anahtar bitleri üretilebilmesi için gerekli şartlar Lemma 1 ile açıklanmıştır.

Lemma 1. $q > 8$ tek tam sayı, $|2\epsilon| = \frac{q}{4} - 2$ iken katsayılar arasındaki ilişki $\|k_{Ai} - k_{Bi}\|_\infty \leq 2\epsilon$ ise ek bilgi $w_{Bi} = Sig(k_{Bi})$ için;
$Mod_2(k_{Ai}, w_{Bi}) = Mod_2(k_{Bi}, w_{Bi})$ eşitliği ile taraflar arasında büyük olasılıkla uzlaşma sağlanır.

Anahtar bileşenler arasındaki farkın belirlenmesine protokolde kullanılan ($2e_i$) hata terimleri ve $\mathbb{Z}_q$'nun parçalanışı etki ederken bu bileşenlerde tahmin edilemezliğin sağlanması ve tarafsız anahtar bitlerinin elde edilmesi için sağlanması gereken şartlar Lemma 2 ile özetlenmiştir.

Lemma 2. $q > 2$ tek tam sayı, eğer $\forall\, k_{Ai} \in \mathbb{Z}_q$'da düzgün rastgele ise $\forall\, w_{Bi} \in \{0,1\}$ için $Mod_2(k_{Ai}, w_{Bi})$ çıktısı düzgün rastgelelik özelliğini sağlar.

Ding17 protokolü ve uzlaşma yöntemi incelendiğinde ortak paylaşılan gizli anahtar üzerinde uzlaşma sağlanırken ek mod işlemlerinin ortadan kaldırılmasıyla iletişim maliyeti azaltılır.

Ayrıca klasik RLWE örnek dağılımından farklı olarak $b = a \cdot s + 2e \; mod \; q$ yaklaşımı ile daha büyük katsayılı hata terimlerinin eklenmesi ile protokolün güvenliği iyileştirilmiştir.

2.2. Peikert14 RLWE Tabanlı Anahtar Paketleme Protokolü

Peikert tarafından 2014 yılında önerilen protokolde kullanılan uzlaşma yönteminde ek bilginin hesaplanmasında $\mathbb{Z}_q$ parçalanışı ve seçilen uzlaşma fonksiyonuna ait işlemlerde farklılaşma gözlemlenmiştir. Bu protokolde yer alan ve birçok protokole temel olan uzlaşma yöntemine ait bileşenlerin açıklanabilmesi amacıyla kullanılan anahtar paketleme protokolü Şekil-3'te özetlenmiştir [11]. Peikert14 anahtar paketleme protokolünde gizli anahtar ve hata terimlerinin üretilmesinde örnekleme $Sample()$ fonksiyonu kullanılırken Ayşe'nin elde ettiği sk_A ve Barış'ın elde ettiği sk_B ortak paylaşılan gizli anahtar değerlerinin yaklaşık olarak eşitliği yuvarlama $\lfloor \cdot \rceil_2$, çapraz yuvarlama $<\cdot>_2$ ve uzlaşma $rec()$ fonksiyonları ile sağlanır. Bu fonksiyonlar uzlaşmanın sağlanmasında $sk_A = sk_B$ anahtar bileşenler hakkında ek bilgi hesaplanmasının yanı sıra parametre seçimlerinde rastgeleliğin garanti edilmesi anlamında faydalar da sağlamaktadır.

Peikert14 protokolü için Tanım 1'de açıklanan RLWE dağılımından anahtar değerlerin üretilmesinde Peikert14 örnekleme fonksiyonu kullanılır.

Tanım 10. Peikert14 Örnekleme Fonksiyonu- $Sample()$: χ; standart sapması σ olan ayrık Gauss dağılımı ya da $\{-B, \cdots, B\}$ aralığında tanımlı düzgün dağılım iken $Sample(\chi)$ ile önerilen protokolde açık anahtar ve gizli anahtar terimleri üretilir.

Peikert14 protokolünde, RLWE probleminin zorluk varsayımının sağlandığı hata terimlerinin (e_i) etkisini azaltmak, $\mathbb{Z}_q$ parçalanışını sağlamak ve tarafsız anahtar bileşenleri üretebilmek amacıyla yuvarlama fonksiyonu kullanılır.

Tanım 11. Yuvarlama Fonksiyonu - $\lfloor \cdot \rceil_p$: Çift q değerleri için $v \in \mathbb{Z}_q$, $p = 2$ olsun. $\lfloor v \rceil_2 = \left\lfloor \frac{2v}{q} \right\rceil$ yuvarlama işlemi ile sağlanan $\mathbb{Z}_q \to \mathbb{Z}_p$ dönüşümü ile v'nin içerdiği hata teriminin etkisi azaltılmaya çalışılır. Yuvarlama fonksiyonu ile $\mathbb{Z}_q$; 0'a yakın bölgeler $I_0 = \{0,1, \cdots, \left\lfloor \frac{q}{4} \right\rceil - 1\}$, $I_1 = \{-\left\lfloor \frac{q}{4} \right\rceil, \cdots, -1\}$ ve 1'e yakın bölgeler $I'_0 = \frac{q}{2} + I_0$ ve $I'_1 = \frac{q}{2} + I_1$ olmak üzere;

$$\begin{cases} 0, & \lceil v \rfloor \in I_0 \;||\; I_1 \\ 1, & \lceil v \rfloor \in I'_0 \;||\; I'_1 \end{cases}$$

eşitliği ile özetlenen 4 bölgeye parçalanır. Bu bölgeler, Ding17 için Tanım 7 ile açıklanan ipucu fonksiyonu ile benzer işlev gerçekleştirir.

Tanım 12. Çapraz Yuvarlama Fonksiyonu - $<\cdot>_2$: Katsayıların tanımlı olduğu $\mathbb{Z}_q$, çapraz yuvarlama fonksiyonu $< v >_2 = \left\lfloor \frac{4v}{q} \right\rceil mod \; 2$ eşitliği ile sağlanan $\mathbb{Z}_q \to \mathbb{Z}_2$ dönüşümü sayesinde v'ye ait ek bilgi olan maske bitinin belirlenmesine olanak sağlar. Örneğin, $v \in I_0$ ise maske biti 0'dır.

Hesaplanan ek bilgi ve uzlaşma fonksiyonu kullanılarak yaklaşık olarak eşit değerlerden aynı en anlamlı bit her iki taraftan da çıkarılarak uzlaşma garanti edilmeye çalışılır.

Tanım 12. Uzlaşma Fonksiyonu - $rec()$: Kriptografik protokollerde q değerinin güvenlik açısından büyük ve asal sayı olması gerekliliği çift q değerleri için tanımlanan Peikert14 uzlaşma işlem adımlarında tek q değerleri için eğilim oluşturmuştur. Bu eğilimin ortadan kaldırılmasında $mod \; 2q$'da çalışılarak geçici ölçeklendirme sağlanmıştır. Geçici ölçeklendirme işleminde $e \in \{0, \pm 1\}$ için $\bar{v} = 2v - e \in \mathbb{Z}_{2q}$ olsun. $\bar{v} \in \mathbb{Z}_{2q}$ katsayısı için ek bilgi $b = < \bar{v} >_2$ iken $E \in \left[\frac{-q}{4}, \frac{q}{4}\right) \cap \mathbb{Z}$ aralığı için uzlaşma fonksiyonu;

$$rec(\bar{v}, b) = \begin{cases} 0, & \bar{v} \in I_b + E \; mod \; 2q \\ 1, & diğer \; durumlar \end{cases}$$

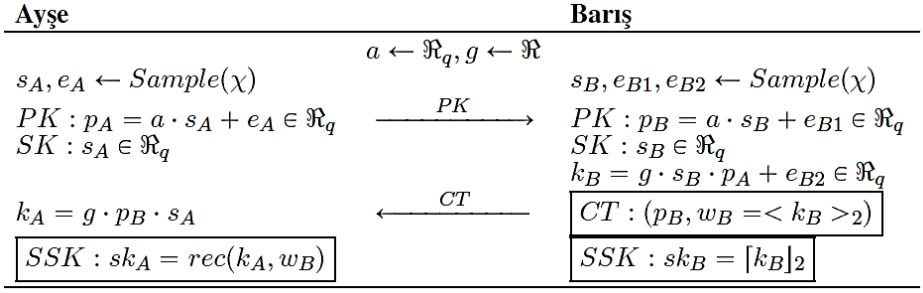
eşitliği ile tanımlanır.

Uzlaşmanın sağlanabilmesi için gerekli koşullar İddia 1 ile açıklanmıştır.

İddia 1. q tek sayı iken $v_2 = v_1 + e \; mod \; q$ olduğu durumda $\bar{e} \in \left[\frac{-q}{4}, \frac{q}{4}\right)$ ve $\overline{v_1} = 2v_1 - \bar{e} \in \mathbb{Z}_{2q}$ ise $2v_2 = \overline{v_1} + (2e + \bar{e}) \; mod \; 2q$ eşitliği ile $\bar{e}$'ın $\frac{1}{2}$ olasılıkla 0, $\frac{1}{4}$ olasılıkla ± 1 olan değerleri için uzlaşma sağlanır.

Ayrıca tek q değerleri için eğer $v \in \mathbb{Z}_q$ 'da düzgün rastgele ise $< \bar{v} >_2$'nin verildiği durumda $\lfloor \bar{v} \rceil_2$ düzgün rastgelelik özelliğini sağlar.

Şekil-3'de açıklanan Peikert14 KEM protokolünde anahtar bileşenler $k_A, k_B \in \Re_q$'dır. Bu bileşenlere ait katsayılar $i \in [n]$ için $k_{Ai}, \; k_{Bi} \in \mathbb{Z}_q$ arasındaki ilişki $w_{Bi} = < k_{Bi} >_2$ için; $|k_{Ai} - k_{Bi}| \leq \frac{q}{4}$ ise $rec(k_A, w_B) = \lfloor k_B \rceil_2$ ile taraflar arasında büyük olasılıkla anahtar paketleme ve çözme işlemi başarıyla gerçekleştirilir.



Şekil-3: Peikert14 RLWE Tabanlı Anahtar Paketleme Protokolü

Peikert14 protokolünde $\mathbb{Z}_q$'ya ait bölgelerin oluşturulmasında q çift ise anahtar tarafsız olurken maske bitleri anahtar hakkında bilgi vermez. Ancak q değerinin yeterince büyük asal olması gerekliliği anahtar bitlerinde bulunan 0 ve 1 değerlerinin dengesizliğiyle ortaya çıkacak olan eğilime neden olur. Bu eğilimi ortadan kaldırmak için $mod\ 2q$ 'da çalışılarak geçici ölçeklendirme yapılır ve küçük miktarda ekstra rastgelelik eklenir. Ayrıca şifre metne ait iki elemandan biri $\Re_q \rightarrow \Re_2$ dönüşümüne uğradığı için şifre metninin uzunluğu $2nlog\ q$ bitten $n(1 + \log q)$ bite indirgenir.

2.3. Saarinen17 RLWE Tabanlı Anahtar Paketleme Protokolü

Saarinen tarafından 2017 yılında önerilen uzlaşma tekniğinde Peikert14 protokolünde çift q değerleri için belirlenen yuvarlama ve ek bilginin elde edilmesi yaklaşımı seçilirken bu yaklaşımın içerdiği eğilimin ortadan kaldırılmasında ve uzlaşmanın sağlanmasında güvenli bölgeden seçim yapma yöntemi kullanılmaktadır. Önerilen bu protokol kuantum bilgisayarlar sonrası güvenilir açık anahtarlı kriptosistem tasarımı sürecinde yer alan Hila5 protokolünün tasarımında kullanılmıştır. Bu protokolde kullanılan uzlaşma yöntemine ait bileşenlerin açıklanabilmesi amacıyla, kullanılan anahtar paketleme protokolü Şekil-4'te özetlenmiştir [6].

Saarinen17 anahtar paketleme protokolünde RLWE dağılımından anahtar değerler üretilirken örnekleme Parse() fonksiyonu kullanılırken Ayşe'nin elde ettiği K ve Barış'ın elde ettiği K′ değerlerinin eşitliğinin sağlanması, $\mathbb{Z}_q$'nun parçalanışının tanımlanması, anahtar bileşene dair ek bilginin üretilmesi ve güvenli bölgeden seçim yapma yaklaşımlarını içeren uzlaşma fonksiyonları SafeBits() ve Select() kullanılır.

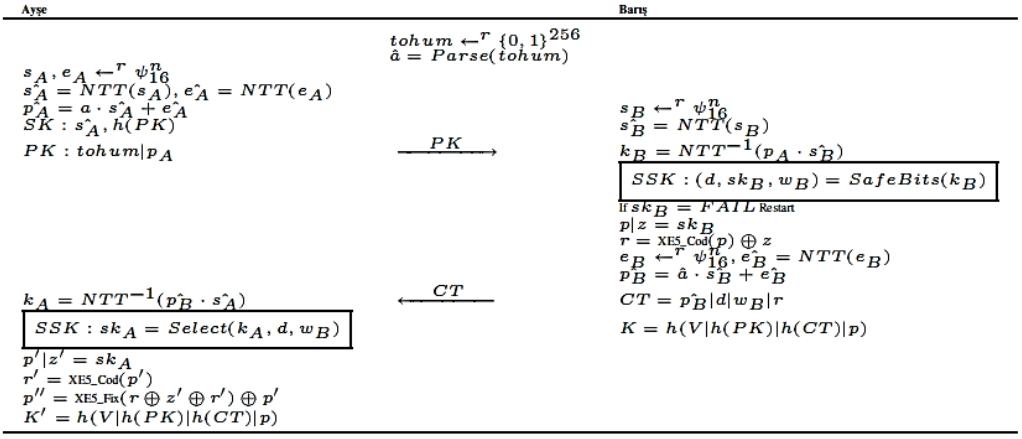
Saarinen17 protokolünde, bu çalışmada ele alınan diğer protokollerden farklı olarak hata terimleri ve gizli terimlerin üretilmesi için binom dağılımı (ψ_{16}^n) kullanılırken Tanım 1'de açıklanan RLWE dağılımından açık anahtarların üretimi için ise Saarinen17 örnekleme fonksiyonu kullanılır.

Tanım 13. Saarinen17 Örnekleme Fonksiyonu - *Parse*(): Taraflar arasında açık anahtarın üretiminde kullanılacak olan a üretecinin belirlenmesinde SHA3'ün XOF modu olan SHAKE-256 kullanılarak üretilen tohum değerine bağlı olarak NTT uzayında düzgün $a \in \Re_q$ açık anahtarı $Parse()$ fonksiyonu ile üretilir. Taraflar arasında güvenli iletişimin sağlanmasında üretilen gizli değerlerin eşitliği için iki farklı uzlaşma fonksiyonu kullanılır.

Tanım 14. Uzlaşma Fonksiyonu1 - *SafeBits*(): Eğilimin ortadan kaldırılmasında Peikert14 protokolünden farklı olarak güvenli bölgelerin oluşturulması yaklaşımını kullanmaktadır. $y \in \Re_q$ anahtar bileşeni için b sınır parametresi iken güvenli bölgelerin oluşturulmasında $i \in [n]$ için;

$$d_i = \begin{cases} 1, & y_i\ mod\ \lfloor \frac{q}{4} \rceil \in \left[\lfloor \frac{q}{8} \rceil - b, \lfloor \frac{q}{8} \rceil + b\right] \\ 0, & diğer\ durumlar \end{cases}$$

eşitliği kullanılarak 4 güvenli bölge oluşturulur. Bu bölgelerde oluşturulacak ortak paylaşılan anahtarın üretiminde Peikert14 protokolünde kullanılan çift q değerleri için belirlenen ek bilgi hesabı $c_i = \left\lfloor \frac{4y_i}{q} \right\rceil\ mod\ 2$ ve tarafsız anahtar bitlerinin üretilebilmesi için gerçekleştirilecek yuvarlama işlemi $k_i = \left\lfloor \frac{2y_i}{q} \right\rceil$ kullanılmaktadır.



Şekil-4: Saarinen17 RLWE Tabanlı Anahtar Paketleme Protokolü

$SafeBits()$ fonksiyonu sonucu elde edilen paylaşılan anahtar bileşene ait ek bilgi c ve d güvenli bölge bitlerinin paylaşımı ile taraflar arasında uzlaşmanın ilk aşaması tamamlanır. İkinci aşama ise gönderici tarafa ait ortak paylaşılan gizli anahtarın $Select()$ fonksiyonuyla belirlenmesidir.

Tanım 15. Uzlaşma Fonksiyonu2 - $Select()$: $SafeBits()$ ile üretilen c ve d değerlerine bağlı olarak gönderici tarafta $x \in \Re_q$ için paylaşılan anahtarın üretilmesi;

$$k'_i = \left\lfloor \frac{2}{q}\left(x_i - c_i \left\lfloor \frac{q}{4} \right\rfloor + \left\lfloor \frac{q}{8} \right\rfloor \ mod\ q\right) \right\rfloor$$

eşitliği ile sağlanır.

Şekil-4'de açıklanan Saarinen17 KEM protokolünde anahtar bileşenler $k_A, k_B \in \Re_q$'dır. Bu bileşenlere ait katsayılar $i \in [n]$ için $k_{Ai}, k_{Bi} \in \mathbb{Z}_q$ arasındaki ilişki $w_{Bi} = \left\lfloor \frac{4k_{Bi}}{q} \right\rfloor mod\ 2$ için;

$|k_{Ai} - k_{Bi}| \leq \frac{q}{4} - b$ ise $SafeBits()$ ve $Select()$ fonksiyonları ile taraflar arasında büyük olasılıkla anahtar paketleme ve çözme işlemi başarıyla gerçekleştirilir.

Önerilen protokol ve uzlaşma yöntemi incelendiğinde paylaşılan gizli anahtar üzerinde uzlaşma sağlanarak şifre metin boyutu ve gereken rastgelelik miktarı azaltılmıştır.

2.4. Hamburg17 MLWE Tabanlı Anahtar Değişim Protokolü

Ding17 ve Saarinen17 protokollerinin yer aldığı kuantum sonrası güvenilir kriptosistem tasarım sürecinde Hamburg, 2017 yılında MLWE problemi tabanlı bir KE protokolü önermiştir. Önerilen bu protokolde yer alan uzlaşma yöntemine ait bileşenlerin açıklanabilmesi amacıyla, kullanılan KE protokolü Şekil-5'te özetlenmiştir [12].

Hamburg17 anahtar değişim protokolünde Ayşe'nin elde ettiği sk_A ve Barış'ın elde ettiği sk_B ortak paylaşılan gizli anahtar değerlerinin eşitliği uzlaşma $recThreebears()$ ve genişletme $use()$ fonksiyonları ile sağlanır. Bu fonksiyonlar ile uzlaşmanın sağlanmasında $sk_A = sk_B$ anahtar bileşen hakkında ek bilgi olarak en anlamlı iki bitin kullanımı yeterli olurken hesaplanan ek bilginin anahtar bileşen hakkında bilgi sızdırmaması ve anahtar bileşende hata teriminin etkisinin azaltılması anlamında faydaları da bulunmaktadır.

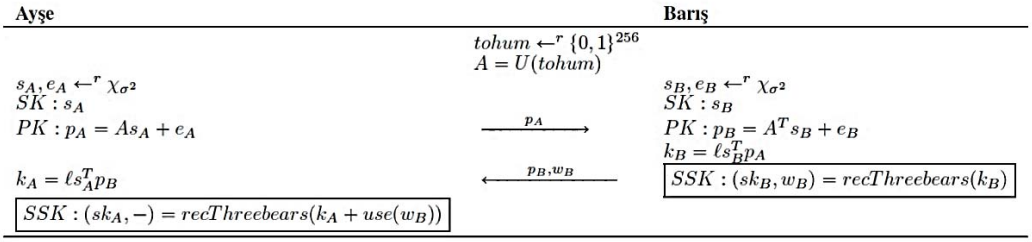
Hamburg17 protokolünde Tanım 2'de açıklanan MLWE dağılımından anahtar değerlerin üretilmesinde Hamburg17 örnekleme fonksiyonu kullanılır.

Tanım 16. Hamburg17 Örnekleme Fonksiyonu – χ_{σ^2}: $d = \{1, \cdots, 4\}$ için $\forall\, e_{i,j} \longleftarrow_r \vartheta_{\sigma^2}$ iken modüller üzerinde tanımlı hata dağılımı;

$$\chi_{\sigma^2} = \left[\sum_{i=0}^{deg(P)-1} e_{i,j} \cdot x^i \right]_{j=0}^{d-1} \in \mathcal{R}^d$$

kullanılarak gizli ve hata terimlerin rastgele seçimi ile MLWE dağılımına bağlı olarak protokolde kullanılacak anahtar değerler oluşturulur.

Hamburg17 protokolünde anahtar bileşenlerin en anlamlı bitlerinde hata teriminin etkisinin en az



Şekil-5: Hamburg17 MLWE Tabanlı Anahtar Değişim Protokolü

olması yaklaşımı ile bu bitlere dayalı uzlaşma yöntemi kullanılır.

Tanım 17. Uzlaşma Fonksiyonu - *recThreebears*(): $\ell \in \mathbb{R}^*$ katsayıların varyansını azaltan bir katsayı iken gizli değer $b \in \chi_{\sigma^2}$, hata terimi $e_B \in \chi_{\sigma^2}$, genel açık anahtar $M = U(tohum) \in \mathcal{R}_q^{dxd}$ iken açık anahtar $A = Ms_A + e_A$ ile hesaplanan anahtar bileşen şu şekilde yazılabilir:

$$C_B = \sum_{i=0}^{deg(P)-1} c_i \cdot x^i \; mod\; q, \;\; c_i \in \mathbb{Z}_q$$

C_B anahtar bileşeni için uzlaşma fonksiyonu ile 2 çıktı elde edilir:

$$recThreebears(C_B) = \begin{cases} (\varpi_B)_i, & c_i \; en\; anlamlı\; bit \\ h_i, & c_i \; en\; anlamlı\; ikinci\; bit \end{cases}$$

Çıktı olarak üretilen $(\varpi_B)_i$ ile ortak paylaşımlı gizli anahtar $sk_B = [\![(\varpi_B)_i]\!]$ iken katsayılara ait ek bilgi ise $w_B = [\![h_i]\!]$'dir.

Hamburg17 protokolünde gönderici tarafta hata terimlerinin (e_i) gönderici tarafa ait anahtar bileşenin en anlamlı ve ikinci en anlamlı bitine olan etkisinin azaltılması ve tahmin edilememezliğin sağlanması amacıyla ek bilgi üzerinde genişletme fonksiyonu kullanılır.

Tanım 18. Genişletme Fonksiyonu - *use*(): Ek bilgi $h \in \mathcal{R}_q$ için;

$$use(h) = \sum_{i=0}^{deg(P)-1} \frac{1 - 2 \cdot h_i}{8} \cdot x^{i+1} \; mod\; q$$

eşitliği ile genişletme fonksiyonu tanımlanır. Bu fonksiyonda $h_i = 1 - 2 \cdot h_i$ yaklaşımı ile anahtar bileşene ait ek bilgi h üzerinde tahmin edilememezlik garanti edilir.

Şekil-5'de özetlenen Hamburg17 KE protokolünde taraflara ait anahtar bileşenler $k_A,\; k_B \in \mathcal{R}_q^d$'dir. Bu bileşenlere ait katsayılar $i \in [d]$ için $k_{Ai}, k_{Bi} \in \mathbb{Z}_q^n$ iken taraflar arasında uzlaşmanın garanti edilebilmesi için gerekli şartlar Lemma 3 ile açıklanmıştır.

Lemma 3. $\epsilon = \frac{q}{8}$ iken katsayılar arasındaki ilişki $|k_{Ai} - k_{Bi}| < \epsilon$ ise ek bilgi $w_{Bi} = use(k_{Bi})$ için;

$$recThreebears(k_{Ai} + w_{Bi}) = recThreebears(k_{Bi})$$

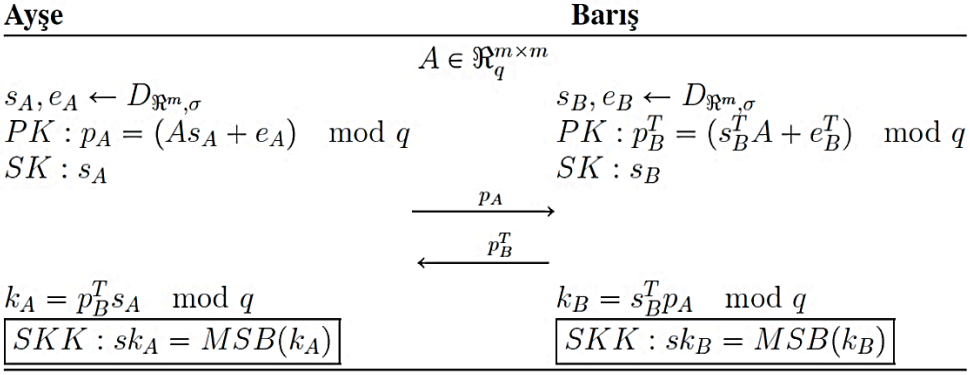
eşitliği ile taraflar arasında büyük olasılıkla uzlaşma sağlanır.

Hamburg17 protokolü ve uzlaşma yöntemi incelendiğinde ortak paylaşılan gizli anahtarın elde edilmesinde polinomlar halkası yerine sözde Mersenne asalları üzerinde tanımlı halka yapısı kullanılmıştır. Ayrıca ortak paylaşımlı gizli anahtarın elde edilmesinde bu çalışmada ele alınan diğer tüm yaklaşımlardan farklı olarak uzlaşma yönteminde katsayılara ait en anlamlı iki bite bağlı uzlaşma yöntemi kullanılmıştır.

2.5. Jing18 Bi-GISIS Tabanlı Anahtar Değişim Protokolü

2018 yılında Jing ve arkadaşları tarafından zorluk varsayımı MLWE problemine denk olan Bi-GISIS problemi tabanlı KE protokolü önerilmiştir. Bu protokolde taraflar arasında eşit ortak paylaşımlı gizli anahtarın elde edilebilmesi için önerilen teknik, uzlaşma fonksiyonu olan MSB ile sınırlandırılmıştır. Bu fonksiyonda taraflara ait anahtar bileşenlerin katsayılarından en anlamsız bitler çıkarılarak ortak paylaşımlı gizli anahtarın elde edilmesi amaçlanır. Uzlaşma yöntemine ait bileşenlerin açıklanabilmesi amacıyla, önerilen KE protokolü Şekil-6'da özetlenmiştir [13].

Jing18 KE protokolünde Tanım 3'de açıklanan Bi-GISIS dağılımından örnekler türetilebilmesi için gizli anahtar ve hata terimlerin üretilmesinde herhangi bir fonksiyon kullanılmadan $\Re^m$'de tanımlı ayrık Gauss dağılımından rastgele seçilerek gerçekleştirilmiştir. Ayrıca Ayşe'nin elde ettiği sk_A ve Barış'ın elde ettiği sk_B ortak paylaşımlı gizli



Şekil-6: Jing18 Bi-GISIS Tabanlı Anahtar Değişim Protokolü

anahtar değerlerinin yaklaşık olarak eşitliği $sk_A = sk_B$ uzlaşma fonksiyonu MSB üzerinde her iki tarafın anlaşması ile sağlanır.

Jing18 protokolünde ortak paylaşılan gizli anahtar değerlerin eşitliğini sağlayan özel bir fonksiyon kullanılmıştır.

Tanım 19. Uzlaşma Fonksiyonu - *MSB*(): $r \in \Re_q$ anahtar bileşenin katsayılarının tanımlı olduğu aralık $r_i < |\frac{q}{2}|$ iken $s = MSB(r)$ fonksiyonu;

$$MSB(r_i) = \begin{cases} s_i = 1, & q/4 < |r_i| < q/2 \\ s_i = 0, & diğer\ durumlar \end{cases}$$

eşitliği ile tanımlanır. Önerilen uzlaşma fonksiyonu ile anahtar bileşenlere ait katsayılardan en anlamlı bit dizisi seçilerek uzlaşmanın sağlanması amaçlanır.

Şekil-6'da açıklanan Jing18 KE protokolünde anahtar bileşenler k_A, $k_B \in \Re_q^m$'dir. Bu bileşenler ile üretilen $sk_A = MSB(k_A)$ ve $sk_B = MSB(k_B)$ değerlerinin eşitliği için gerekli şartlar Lemma 4 ile özetlenmiştir.

Lemma 4. $m \geq 2$ sabit sayı, $\lambda = O(n)$, $\beta = \sqrt{n}\sigma$, $q = O(2^{\lambda} mn\beta^2)$ iken $i \in [m]$ için $\|e_{Ai}\| < \sqrt{n}\sigma = \beta$, $\|e_{Bi}\| < \sqrt{n}\sigma = \beta$, $\|s_{Ai}\| < \sqrt{n}\sigma = \beta$, $\|s_{Bi}\| < \sqrt{n}\sigma = \beta$ ise $\|e_B^T s_A\| \leq mn\beta^2$ ve $\|e_A s_B^T\| \leq mn\beta^2$'dır.

$$k_A = p_B^T s_A \mod q = (s_B^T A + e_B^T) s_A \mod q$$
$$= s_B^T A s_A + e_B^T s_A \mod q$$
$$k_B = s_B^T p_A \mod q = s_B^T (A s_A + e_A) \mod q$$
$$= s_B^T A s_A + s_B^T e_A \mod q$$

eşitliklerinde $\|s_B^T A s_A\| \approx q$ iken sınırları Lemma 4 ile açıklanan MSB fonksiyonu sonucu elde edilen sk_A, sk_B değerlerinin tüm katsayılarında en anlamlı λ bit $O(n2^{-\lambda})$ olasılıkla eşit olacağı için ortak paylaşılan anahtar üzerinde uzlaşma sağlanır.

Jing18 KE protokolünde yer alan uzlaşma yönteminde ek bilgi hesabı kullanılmamaktadır. Ancak, uzlaşma fonksiyonu içerisinde anahtar bileşenlerden en anlamlı bit dizisinin seçilmesinde $\mathbb{Z}_q$, 3 bölgeye parçalanmıştır. Dolayısıyla, bu uzlaşma yöntemi için gözlemlenen temel farklılaşma seçilen zor problemin değişmesi ve ek bilgiye ihtiyaç duyulmadan gerçekleştirilen uzlaşma yapısıdır.

3. Sistemlerin Karşılaştırılması

Bu çalışmada ele alınan Ding17, Peikert14, Saarinen17, Hamburg17 ve Jing18 KE\KEM protokollerinde uzlaşma problemi için önerilen yöntemler içerdikleri işlem adımlarının çalışma yapısı ve sayısına bağlı olarak içermiş oldukları benzerlikler ve farklılıklar genel bakış açısı verecek şekilde Çizelge-1'de özetlenmiştir. Ayrıca yuvarlama işleminin varlığı ve $\mathbb{Z}_q$ parçalanışına bağlı olarak ek bilginin nasıl hesaplandığı gibi temel işlem adımlarının yanı sıra protokollerde kullanılan zor problem yapısı, hata uzlaşmasında kullanılan fonksiyon sayısı, uzlaşma şartları ve parametre seçimleri açısından detaylı bir karşılaştırma Çizelge-2 ile özetlenmiştir.

- ***Yuvarlama İşlemi:*** Kafes tabanlı zor problemlerin yapısında bulunan hata terimleri KE protokollerinde aynı paylaşılan gizli anahtarın elde edilememesine neden olurken KEM protokollerinde şifre çözmede başarısızlık oluşması ihtimalini ortaya çıkarır. Diğer terimlere göre oldukça küçük seçilen hata terimlerinin etkisinin ortadan kaldırılması amacıyla yuvarlama işlemi kullanılmaktadır.

Çizelge-1: Seçilen Anahtar Değişim/Paketleme Protokollerinin Uzlaşma İşlem Adımları Açısından Karşılaştırılması

	Tür	Yuvarlama	Ek Bilgi	$\mathbb{Z}_q$'nun Parçalanışı	Varsayım	Uzlaşma Fonksiyonu Sayısı
Ding17	*KE*	✓	✓	✓	RLWE	*1*
Peikert14	*KEM*	✓	✓	✓	RLWE	*2*
Saarinen17	*KEM*	✓	✓	✓	RLWE	*2*
Hamburg17	*KE*	×	✓	×	MLWE	*1*
Jing18	*KE*	×	×	✓	Bi-GISIS	*1*

KE: Anahtar Değişim, KEM: Anahtar Paketleme

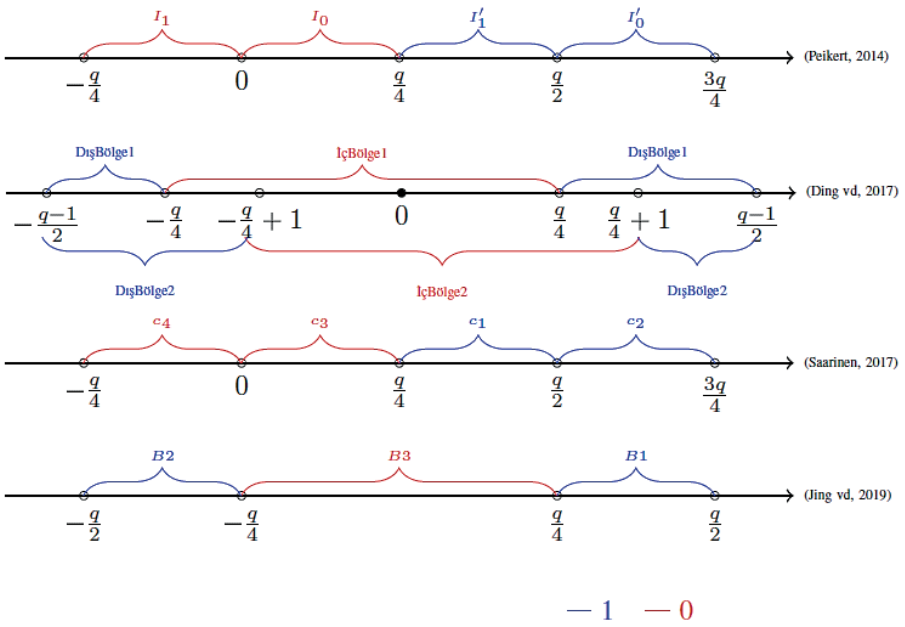
- Bu çalışmada ele alınan Ding17, Peikert14 ve Saarinen17 protokollerinde yuvarlama işlemi yaklaşımı kullanılarak hata terimlerinin etkisinin azaltılmasını amaçlarken Hamburg17 ve Jing18 protokollerinde doğrudan yuvarlama işlemi kullanılmamaktadır.

- $\mathbb{Z}_q$***'nun Parçalanışı*:** Uzlaşma probleminin ortadan kaldırılmasında kullanılan ara işlem adımlarından biri de ek bilginin gönderilmesidir. Gönderilecek olan ek bilginin hesaplanmasında ise genellikle katsayının $\mathbb{Z}_q$'da bulduğu bölgeye bağlı olarak belirlenen değerler ile işlemler yapılmaktadır. Bu çalışmada ele alınan Ding17, Peikert14 ve Saarinen17 protokolleri ek bilgi hesabında $\mathbb{Z}_q$'nun parçalanışı yaklaşımını kullanırken Jing18 protokolünde ise uzlaşma fonksiyonu içerisinde $\mathbb{Z}_q$'nun parçalanışı yaklaşımı kullanılmaktadır. Hamburg17 protokolü ise ek bilgi gönderme yaklaşımını kullansa da özelleşmiş bir $\mathbb{Z}_q$ parçalanışına sahip değildir. Ding17, Peikert14, Saarinen17 ve Jing18 protokolleri için belirlenen $\mathbb{Z}_q$'nun parçalanışı yaklaşımları Şekil-7'de özetlenmiştir. Ayrıca $\mathbb{Z}_q$'nun parçalanışı protokollerde üretilen anahtar bileşenler için üst sınır oluşturacağından bu özellik parametre seçim kümelerini de etkilemektedir.

- ***Ek Bilgi Hesabı:*** Ek bilgi, anahtar bileşene ait katsayının $\mathbb{Z}_q$'nun parçalanışına bağlı olarak belirlenen bölgelerde bulunması durumları ele alınarak hesaplanmaktadır. KE\KEM protokollerinde yer alan alıcı tarafa ait ek bilginin hesaplanması ve gönderici tarafın bu bilgiye bağlı olarak kendi paylaşılan gizli anahtarını hesaplaması ile aynı paylaşılan gizli anahtar elde edilir. Bu çalışmada ele alınan Jing18 protokolü ek bilgi hesabı yaklaşımını kullanmazken Ding17, Peikert14 ve Saarinen17 protokolleri $\mathbb{Z}_q$'nun parçalanışına bağlı olarak ek bilgi hesabı ve Hamburg17 protokolü ise en anlamlı bitlere bağlı ek bilgi hesabı yaklaşımlarını kullanmaktadır. Bu durum ek bilgi kullanan ve kullanmayan iki farklı uzlaşma yöntemi yapısının oluşturulabileceğini açıklamaktadır.

- ***Uzlaşma Fonksiyonu:*** Uzlaşma problemi için sunulan ara işlem adımların tamamlanması sonucunda tarafların aynı paylaşılan gizli anahtarı üretebilmesi uzlaşma fonksiyonu ile garanti edilir. Bu çalışmada ele alanın Ding17, Hamburg17 ve Jing18 protokolleri tek bir uzlaşma fonksiyonu kullanırken Peikert14 ve Saarinen17 protokolleri ise iki farklı uzlaşma fonksiyonu kullanılmaktadır.

- ***Yeni Yaklaşım:*** Bu çalışma ile parametrelerin seçimine bağlı olarak ek bilgi kullanılmadan da uzlaşma problemine çözüm önerisi sunulabileceği gözlemlenmiştir. Bu yaklaşım ile anahtar bileşende yer alan katsayıların tek veya çift sayı olma özelliğini temel alan, bir veya daha fazla ek bilgi biti içeren veya hiç ek bilgi kullanılmayan, $\mathbb{Z}_q$ parçalanışında 4 veya 4'den daha fazla bölge oluşumuna sahip, farklı zor problemlerin özelliklerini temel alan, yuvarlama işlemi ile hata terimlerinin etkisinin azaltıldığı yaklaşımlarını içeren uzlaşma yöntemlerinin uygunluğunun analizi planlanmaktadır.



Şekil-4: Ding17, Peikert14,Saarinen17 ve Jing18 Protokollerinde Kullanılan $\mathbb{Z}_q$ Parçalanış Şekilleri

4. Sonuçlar ve Öneriler

Bu çalışmada kuantum bilgisayarlar sonrası kriptografi için önerilen bazı kafes tabanlı KE\KEM protokolleri ele alınarak genel bir bakış açısı verecek şekilde işleyiş adımları açıklanmıştır. Bu yaklaşım ile kafes tabanlı KE\KEM protokolleri için açık problem [8] olarak ifade edilen uzlaşma yöntemlerine çözüm önerisi sunabilmek için bilgi birikiminin oluşturulması hedeflenmiştir. [9] nolu çalışmada yer alan protokollere ek olarak 2 farklı yaklaşımın yer aldığı KE\KEM protokollerinde kullanılan uzlaşma yöntemleri arasındaki farklılıklar analiz edilerek yeni bir uzlaşma yönteminin içermesi gereken adımlar belirlenmiştir. Bu adımlar belirlenirken protokollerde kullanılan cebirsel yapıya bağlı olarak yuvarlama işlemi, ek bilgi hesabı, $\mathbb{Z}_q$'nun parçalanışı ve uzlaşma fonksiyonu sayısı ve yapısı analiz edilmiştir. Bu özelliklerin neticesinde önerilebilecek yeni uzlaşma yönteminin genel yapısı açıklanmıştır. Belirlenen yaklaşımın içermesi gereken fonksiyonlara ait içeriklerin belirlenmesi ve buna bağlı olarak kafes tabanlı KE\KEM protokollerinin önerilmesi gelecekte yapılması planlanan çalışmalar olarak belirlenmiştir.

5. Bilgilendirme

EEEAG-117E636 proje numarası ile TÜBİTAK tarafından desteklenen bu çalışma [9] nolu çalışmanın genel bir yapıya uyarlanmış halidir.

Çizelge-2: Ding17, Peikert14, Saarinen17, Hamburg17 ve Jing18 Anahtar Değişim/Paketleme Protokollerinde Kullanılan Uzlaşma Yapılarının Karşılaştırılması

	Ding17	**Peikert14**	**Saarinen17**	**Hamburg17**	**Jing18**
Kullanılan Örnek Dağılımı	$b = a \cdot s + 2e \in \Re_q$	$b = a \cdot s + e \in \Re_q$	$b = a \cdot s + e \in \Re_q$	$b = a \cdot s + e \in R_q^d$	$b_1 = As_1 + e_1 \in \Re_q^m$ $b_2^T = s_2^T A + e_2^T \Re_q^m$
Zorluk Varsayımı	RLWE (bkz. Tanım 1)	RLWE (bkz. Tanım 1)	RLWE (bkz. Tanım 1)	M-LWE (bkz. Tanım 2)	Bi-GISIS (bkz. Tanım 3)
Cebirsel Yapı	$\Re_q = \mathbb{Z}_q[x]/(x^n + 1)$	$\Re_q = \mathbb{Z}_q[x]/(x^n + 1)$	$\Re_q = \mathbb{Z}_q[x]/(x^n + 1)$	$N = 2^{3120} - 2^{1560} - 1$ sözde-Mersenne asalı $R^d = (\mathbb{Z}_q[x]/N)^d$	$\Re_q^m = (\mathbb{Z}_q[x]/(x^n + 1))^m$
Hata Dağılımı	$D_{\mathbb{Z}^n,\sigma}$	χ	ψ_{16}^n	χ_{σ^2}	$D_{\Re^m,\sigma}$
Yuvarlama	$\lfloor x\frac{p}{q} \rceil$, p=7551 (bkz. Tanım 5)	$\lfloor \frac{pv}{q} \rceil$, p=2 (bkz. Tanım 11)	$\lfloor \frac{2y_i}{q} \rfloor$ (bkz. Tanım 14)	-	-
Ek Bilgi	✓ Ek bilgi bitleri; sinyal bitleri. ✓ Katsayı hangi bölgede bilgisi ile hesaplanır. ✓ $\mathbb{Z}_q \to \mathbb{Z}_2$ sağlanır. ✓ $\mathbb{Z}_q$, etiketi $\{0, 1\}$ olan 4 bölge. ✓ Sinyal bitleri 2 bölge için 1, kalan iki bölge için 0 olarak etiketlenir. ✓ Her bir katsayı için bir sinyal biti. (bkz. Tanım 7-Tanım 8)	✓ Ek bilgi bitleri; sinyal bitleri. ✓ Katsayı hangi bölgede bilgisi ile hesaplanır. ✓ $\mathbb{Z}_q \to \mathbb{Z}_2$ sağlanır. ✓ $\mathbb{Z}_q$, etiketi $\{0, 1\}$ olan 4 bölge. ✓ Maske bitleri 0'a yakın bölgeler için 0, kalan iki bölgede 1. ✓ Her bir katsayı için bir maske biti. (bkz. Tanım 11)	✓ Peikert14 çift q için ek bilgi biti hesabı yaklaşımı. ✓ Katsayı hangi bölgede bilgisi ile hesaplanır. ✓ $\mathbb{Z}_q \to \mathbb{Z}_2$ sağlanır. ✓ $\mathbb{Z}_q$, etiketi $\{0, 1\}$ olan 4 bölge. ✓ Ek bilgi bitleri 2 bölge için 1, kalan iki bölge için 0 olarak etiketlenir. ✓ Her bir katsayı için bir ek bilgi biti. (bkz. Tanım 14)	✓ Ek bilgi olarak katsayının ikinci en anlamlı biti seçilir. ✓ İkinci en anlamlı bit dizisi oluşturulur. (bkz. Tanım 17)	-
$\mathbb{Z}_q$ Parçalanışı	İç Bölge1: $[-\lfloor \frac{q}{4} \rfloor, \lfloor \frac{q}{4} \rfloor]$ İç Bölge2: $[-\lfloor \frac{q}{4} \rfloor + 1, \lfloor \frac{q}{4} \rfloor + 1]$ Dış Bölge1: $\mathbb{Z}_q \setminus [-\lfloor \frac{q}{4} \rfloor, \lfloor \frac{q}{4} \rfloor]$ Dış Bölge2: $\mathbb{Z}_q \setminus [-\lfloor \frac{q}{4} \rfloor + 1, \lfloor \frac{q}{4} \rfloor + 1]$ (bkz. Tanım 7)	$I_0 : [0, \lfloor \frac{q}{4} \rceil - 1]$ $I_1 : [-\lfloor \frac{q}{4} \rceil, -1]$ $I'_0 : \frac{q}{2} + I_0$ $I'_1 : \frac{q}{2} + I_1$ (bkz. Tanım 11)	$c1 : [\frac{q}{4}, \frac{q}{2})$ $c2 : [\frac{q}{2}, \frac{3q}{4})$ $c3 : [0, \frac{q}{4})$ $c4 : [-\frac{q}{4}, 0)$ (bkz. Tanım 14)	-	B1: $q/4 < r_i < q/2$ B2: $-q/2 < r_i < -q/4$ B3: $\mathbb{Z}_q \setminus \{B1 \cup B2\}$ (bkz. Tanım 19)
Hatada Uzlaşma	sig() ve $\text{Mod}_2()$	$<>_2$, $\lfloor \rceil_2$, rec()	Güvenli bölge seçimi $(SafeBits(), Select())$	recThreebears(), use()	MSB()
Yaklaşık Uzlaşma	Yuvarlama Sinyal gönderme	Yuvarlama Maske bitleri gönderme	Yuvarlama Ek bigiye dayalı güvenli bölgeden seçim	Genişletme, En anlamlı ve ikinci en anlamlı bite dayalı uzlaşma.	-
Uzlaşma Şartı	$x = y + 2\varepsilon$ $\|x - y\|_\infty \leq \frac{q}{4} - 2$ (bkz. Lemma1)	$2x = \bar{y} + (2e + \bar{e})$ $\|x - y\| < \frac{q}{4}$ (bkz. İddia 1)	$\|x - y\| \leq \frac{q}{4} - b$, b=799 (bkz. Tanım 15)	$\|x - y\| < \frac{q}{8}$ (bkz. Lemma 3)	(bkz. Lemma 4)
Parametre Seçimleri [16]	128-bit güvenlik seviyesi: (n,σ,q)=(512, 4.19, 120833) 192, 256-bit güvenlik seviyesi: (n,σ,q)=(1024, 2.6, 120833)	-	256-bit güvenlik seviyesi: (n,σ,q)=(1024, 2.83, 12289)	PapaBear 256-bit güvenlik seviyesi: (n,σ,q)=(1248, 0.61, 1024)	-
Diğer Özellikler	✓ DH benzeri KE. ✓ Ek mod işlemlerinden kurtulma. ✓ Düşük iletişim maliyeti. ✓ Hata terimi ($2e$) ile daha güvenli. ✓ Tarafsız anahtar bitleri.	✓ DH benzeri aktif/pasif KEM ✓ Tarafsız ve düzgün anahtar ✓ Şifre metni uzunluğu ($n(1 + \log q)$)	✓ DH benzeri aktif ve güvenli KEM. ✓ Şifre metin uzunluğu ($> n(1 + \log q)$). ✓ Daha az rastgelelik. ✓ Küçük hata oranı. ✓ İki farklı uzlaşma fonksiyonu.	✓ DH benzeri KE. ✓ En anlamlı 2 bite dayalı uzlaşma. ✓ Farklı cebirsel yapı.	✓ DH benzeri KE ✓ $O(n2^{-\lambda})$ olasılıkla uzlaşmanın sağlanması

Kaynakça

[1] Diffie, W., Hellman, M., *New Directions in Cryptography,* IEEE Transactions on Information Theory, vol. 22 (6), 1976, pp. 644--654.

[2] Shor, P.W., *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, In Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE, 1994, pp. 124--134.

[3] De Wolf, R., *Quantum Computing: Lecture Notes*, arXiv preprint arXiv:1907.09415, 2019, pp. 1--11.

[4] NIST Post-Quantum Cryptography Standardization Project, https://csrc.nist.gov/projects/post-quantumcryptography (Erişim Tarihi: 21.10.2019)

[5] Bernstein, D. J., Buchmann, J., Dahmen, E., *Post-Quantum Cryptography*, 1st ed., Springer, 2008, pp. 1--13.

[6] Saarinen, M.J.O., *Hila5*, Technical Report, National Institute of Standards and Technology (NIST), 2017.

[7] Gao, X., *Comparison Analysis of Ding's RLWE-Based Key Exchange Protocol and NewHope Variants*, Advances in Mathematics of Communications, vol. 13 (2), 2019, pp. 221--233.

[8] Alperin-Sheriff, J., *Suggested Avenues for Lattice-Based Research*, In Lattice Crypto and Algorithms, University Residential Center, Italy, 2018.

[9] Akleylek, S., Seyhan, K., *Kafes-Tabanlı Anahtar Değişim/Paketleme Protokollerinde Kullanılan Uzlaşma Yöntemleri*, The 4th International Conference on Computer Science and Engineering (UBMK'19), IEEE, 2019, pp. 91--96.

[10] Ding, J., Takagi, T., Gao, X., Wang, Y., *Ding Key Exchange*, Technical Report, National Institute of Standards and Technology (NIST), 2017.

[11] Peikert, C., *Lattice Cryptography for the Internet*, Post-Quantum Cryptography, Springer, LNCS, vol. 8772, 2014, pp. 197--219.

[12] Hamburg, M., *Module-LWE Key Exchange and Encryption: The Three Bears*, Technical Report, National Institute of Standards and Technology (NIST), 2017.

[13] Jing, Z., Gu, C., Yu, Z., Shi, P., Gao, C., *Cryptanalysis of Lattice-based Key Exchange on Small Integer Solution Problem and its Improvement*, Cluster Computing, vol. 22 (1), 2019, pp. 1717--1727.

[14] Lyubashevsky, V., Peikert, C., Regev, O., *On Ideal Lattices and Learning with Errors Over Rings,* Advances in Cryptology – EUROCRYPT 2010, LNCS, vol. 6110, 2010, pp. 1--23.

[15] Langlois, A., Stehle, D., *Worst-case to average-case reductions for module lattices*, Designs, Codes and Cryptography, vol. 75 (3), 2015, pp. 565--599.

[16] Albrecht, M. R., et al., *Estimate All the {LWE, NTRU} Schemes!*, Security and Cryptography for Networks, SCN 2018, LNCS, vol. 11035, 2018, pp. 351--367.