KRİPTOLOJİ VE EN YAYGIN KULLANILAN KRİPTOGRAFİK ALGORİTMALAR

Bölüm II: Sertifika altyapısı, protokoller, anahtar yönetimi, kuantum sonrası geçiş ve hukuki çerçeve

Cryptology and the Most Widely Used Cryptographic Algorithms, Part II: Certificate Infrastructure, Protocols, Key Management, the Post-Quantum Transition and the Legal Framework

Derleme Makale / Review Article

Dr. Burak Olgun
burakolgun@solutionhome.net
Solution Home Bilişim Tekn. ve Dan. Hizm., İstanbul

Açık Anahtar Altyapısı • Sertifika Şeffaflığı • TLS 1.3 • Anahtar Yönetimi • ML-KEM • Kuantum Sonrası Kriptografi • KVKK • CMK m. 134

ÖZET

İki bölümlük serinin bu ikinci makalesi, birinci bölümde incelenen kriptografik algoritmaların gerçek sistemlerde nasıl bir araya getirildiğini ve bu sistemleri önümüzdeki on yılda nelerin beklediğini ele almaktadır. İlk olarak X.509 sertifika altyapısı, güven zinciri, DigiNotar ve TÜRKTRUST olayları, Sertifika Şeffaflığı, Let's Encrypt ile gelen otomasyon, 2029'da 47 güne inecek sertifika ömrü ve WebAuthn geçiş anahtarları incelenmektedir. Ardından TLS 1.3, SSH, Signal, WPA3, disk şifreleme, elektronik imza ve blokzincir protokollerinin hangi algoritmaları nerede kullandığı gösterilmekte; rastgele sayı üretimi (NIST SP 800-90A/B/C), anahtar yaşam döngüsü, donanım güvenlik modülleri ve FIPS 140-3 ele alınmaktadır. Kuantum tehdidi bölümünde Shor ve Grover algoritmaları, NIST'in FIPS 203, 204 ve 205 standartları, hibrit X25519MLKEM768 anahtar değişimi, boyut kaynaklı geçiş güçlükleri ve ABD, Birleşik Krallık ile AB geçiş takvimleri karşılaştırılmaktadır. Homomorfik şifreleme, sıfır bilgi ispatları ve güvenli çok taraflı hesaplama ile Clipper çipinden AB "sohbet denetimi" teklifine uzanan yasal erişim tartışması da değerlendirilmektedir. Türkiye bağlamı 5070 sayılı Elektronik İmza Kanunu, 6698 sayılı KVKK, 7545 sayılı Siber Güvenlik Kanunu ve Anayasa Mahkemesi'nin 2026'da iptal ettiği CMK m. 134 çerçevesinde ortaya konulmakta; Türkiye için ilan edilmiş bir kuantum sonrası geçiş takviminin bulunmadığı tespit edilmektedir. Makale, kriptografik envanter, kripto çeviklik ve sertifika otomasyonuna dayalı somut önerilerle sona ermektedir.

Anahtar Kelimeler: *açık anahtar altyapısı, X.509, sertifika şeffaflığı, TLS 1.3, Signal protokolü, WebAuthn, rastgele sayı üretimi, anahtar yönetimi, FIPS 140-3, kuantum sonrası kriptografi, ML-KEM, ML-DSA, homomorfik şifreleme, sıfır bilgi ispatı, yasal erişim, elektronik imza, KVKK, CMK m. 134*

ABSTRACT

This second article of a two-part series examines how the cryptographic algorithms covered in the first part are combined in real systems and what awaits these systems in the coming decade. It first examines the X.509 certificate infrastructure, the chain of trust, the DigiNotar and TÜRKTRUST incidents, Certificate Transparency, the automation brought by Let's Encrypt, the reduction of certificate lifetimes to 47 days by 2029 and WebAuthn passkeys. It then shows which algorithms TLS 1.3, SSH, Signal, WPA3, disk encryption, electronic signatures and blockchains use and where, and addresses random number generation (NIST SP 800-90A/B/C), the key life cycle, hardware security

burakolgun.com

modules and FIPS 140-3. The quantum section compares Shor's and Grover's algorithms, NIST's FIPS 203, 204 and 205 standards, hybrid X25519MLKEM768 key exchange, size-related migration difficulties and the US, UK and EU migration timelines. Homomorphic encryption, zero-knowledge proofs and secure multi-party computation are assessed, together with the lawful access debate from the Clipper chip to the EU "chat control" proposal. The Turkish context is set out under the Electronic Signature Law No. 5070, the Personal Data Protection Law No. 6698, the Cybersecurity Law No. 7545 and Article 134 of the Code of Criminal Procedure, annulled by the Constitutional Court in 2026, and the absence of an announced national post-quantum migration timeline is noted. The article closes with concrete recommendations based on cryptographic inventory, crypto-agility and certificate automation.

Keywords: *public key infrastructure, X.509, certificate transparency, TLS 1.3, Signal protocol, WebAuthn, random number generation, key management, FIPS 140-3, post-quantum cryptography, ML-KEM, ML-DSA, homomorphic encryption, zero-knowledge proof, lawful access, electronic signature, personal data protection*

1. Giriş

Serinin birinci bölümünde AES, ChaCha20, SHA-2, RSA ve eliptik eğri algoritmaları tek tek incelenmiş ve gerçek dünyadaki kırılmaların çoğunun algoritmalardan değil, onların nasıl kullanıldığından kaynaklandığı gösterilmişti. Bu ikinci bölüm tam da o "nasıl" sorusuna odaklanmaktadır. Bir algoritma tek başına hiçbir şeyi korumaz. Bir web sitesine güvenli bağlanabilmek için açık anahtarın gerçekten o siteye ait olduğunun kanıtlanması, anahtar değişiminin bir protokol içinde doğru sırayla yapılması, kullanılan rastgele sayıların gerçekten tahmin edilemez olması ve anahtarların yaşam döngüsü boyunca korunması gerekir. Bu halkaların her biri, son on beş yılın büyük güvenlik olaylarından en az birinde kopmuştur.

2024 yılı alan için yeni bir dönemin de başlangıcıdır. ABD Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology, NIST), sekiz yıl süren açık bir yarışmanın sonunda kuantum bilgisayarlara dayanıklı ilk üç standardı (FIPS 203, 204 ve 205) yayımlamıştır (NIST, 2024a, 2024b, 2024c). Büyük tarayıcılar ve içerik dağıtım ağları hibrit kuantum sonrası anahtar değişimini varsayılan hâle getirmiş, Cloudflare 2025 sonunda insan kaynaklı trafiğinin yarısından fazlasının bu yöntemle korunduğunu bildirmiştir (Westerbaan, 2025). Aynı dönemde sertifika ömürlerinin kısaltılması, FIPS 140-2'den FIPS 140-3'e geçiş ve Türkiye'de Anayasa Mahkemesi'nin dijital delillere ilişkin CMK m. 134'ü iptal etmesi, kriptografinin hem teknik hem hukuki çerçevesini aynı anda değiştirmektedir.

Bu bölümün geri kalanı şu şekilde düzenlenmiştir. İkinci kısım açık anahtar altyapısını ve sertifikaları, üçüncü kısım algoritmaların TLS 1.3, SSH, Signal ve diğer protokollerde nasıl birleştiğini, dördüncü kısım rastgele sayı üretimini ve anahtar yönetimini ele almaktadır. Beşinci kısım kuantum tehdidini, NIST standartlarını ve ulusal geçiş takvimlerini, altıncı kısım homomorfik şifreleme ve sıfır bilgi ispatı gibi ileri yapıları, yedinci kısım şifreleme politikası ve yasal erişim tartışmasını incelemektedir. Sekizinci kısım hukuki çerçeveyi ve Türkiye bağlamını, dokuzuncu kısım önerileri, onuncu kısım sonuçları içermektedir.

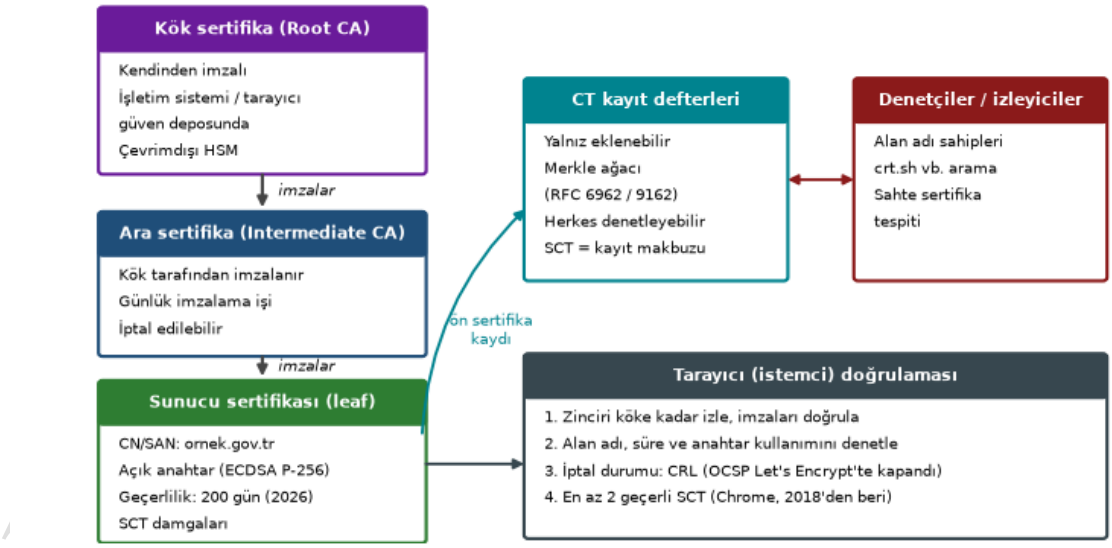
burakoguz.com

2. Açık Anahtar Altyapısı ve Sertifikalar

2.1. X.509 Sertifikaları ve Güven Zinciri

Açık anahtarlı kriptografi bir soruyu cevapsız bırakır: elimdeki açık anahtarın gerçekten konuşmak istediğim kişiye ait olduğunu nereden bileceğim? Araya giren bir saldırgan kendi açık anahtarını banka adına sunabilir. **Açık anahtar altyapısı (Public Key Infrastructure, PKI)** bu soruyu, güvenilen üçüncü tarafların imzaladığı sertifikalarla cevaplar. Web ve e-imza dünyasında kullanılan biçim, profili RFC 5280 ile tanımlanan **X.509 v3** sertifikasıdır (Cooper vd., 2008). Bir sertifika temelde sahibin kimliğini (alan adı veya kişi), açık anahtarını, geçerlilik süresini ve kullanım kısıtlarını bir araya getirir ve bu paketi bir sertifika otoritesinin (Certificate Authority, CA) imzasıyla bağlar.

Şekil 1'de görüldüğü gibi güven hiyerarşiktir. İşletim sistemleri ve tarayıcılar, kök sertifika deposunda birkaç yüz kök CA sertifikası taşır. Kök anahtarlar genellikle çevrimdışı donanım güvenlik modüllerinde tutulur ve yalnızca ara sertifikaları imzalamak için kullanılır. Günlük imzalama işini ara CA'lar yapar. Tarayıcı, sunucu sertifikasından başlayarak her imzayı bir üst sertifikanın açık anahtarıyla doğrular ve zinciri güvendiği bir köke ulaştırabiliyorsa bağlantıyı kabul eder. Bu yapının zayıf noktası da buradadır: güvenilen yüzlerce CA'dan herhangi biri, dünyadaki herhangi bir alan adı için geçerli görünen bir sertifika üretebilir.



Kaynak: RFC 5280 (Cooper vd., 2008), RFC 6962 (Laurie vd., 2013), RFC 9162 ve Let's Encrypt (2025) temel alınarak derlenmiştir.

Şekil 1. X.509 güven zinciri ve Sertifika Şeffaflığı (CT) denetim mekanizması

2.2. Sertifika Otoritesi İhlalleri: DigiNotar ve TÜRKTRUST

Bu riskin en ağır örneği Hollandalı DigiNotar vakasıdır. Fox-IT'in resmi inceleme raporuna göre saldırganlar 17 Haziran 2011'de şirketin ağına sızmış, 10 Temmuz'da ilk sahte sertifikayı üretmiş ve toplam 531 sahte sertifika tespit edilmiştir. Bunlar arasında *.google.com için üretilen sertifika, Gmail trafiğinin ortadaki adam saldırısıyla okunmasında kullanıldı. Sahte sertifika için yapılan OCSP sorgularının 298.140 farklı IP adresinden geldiği ve bunların

%95'inin İran kaynaklı olduğu belirlendi (Hoogstraaten vd., 2012). Olay, Chrome'un sertifika sabitleme (pinning) özelliği sayesinde fark edildi; DigiNotar tüm tarayıcıların güven deposundan çıkarıldı ve aynı yıl iflas etti.

Türkiye'den de ders çıkarılacak bir örnek vardır. Google'ın 3 Ocak 2013 tarihli açıklamasına göre Chrome, 24 Aralık 2012 gecesi *.google.com için yetkisiz bir sertifikayı engellemiş; incelemede TÜRKTRUST'ın Ağustos 2011'de iki müşterisine yanlışlıkla son kullanıcı sertifikası yerine ara CA sertifikası** verdiği anlaşılmıştır. Yetkisiz Google sertifikası bu ara sertifikalardan biriyle üretilmişti (Langley, 2013). Mozilla iki ara sertifikayı iptal etti ve Firefox güncellemesini 8 Ocak 2013'te yayımladı (Mozilla, 2013). Olayın kötü niyetli bir saldırıdan değil süreç hatasından kaynaklanması, PKI'da tek bir idari hatanın küresel sonuç doğurabileceğini göstermesi bakımından öğreticidir.

2.3. Sertifika Şeffaflığı ve Otomasyon

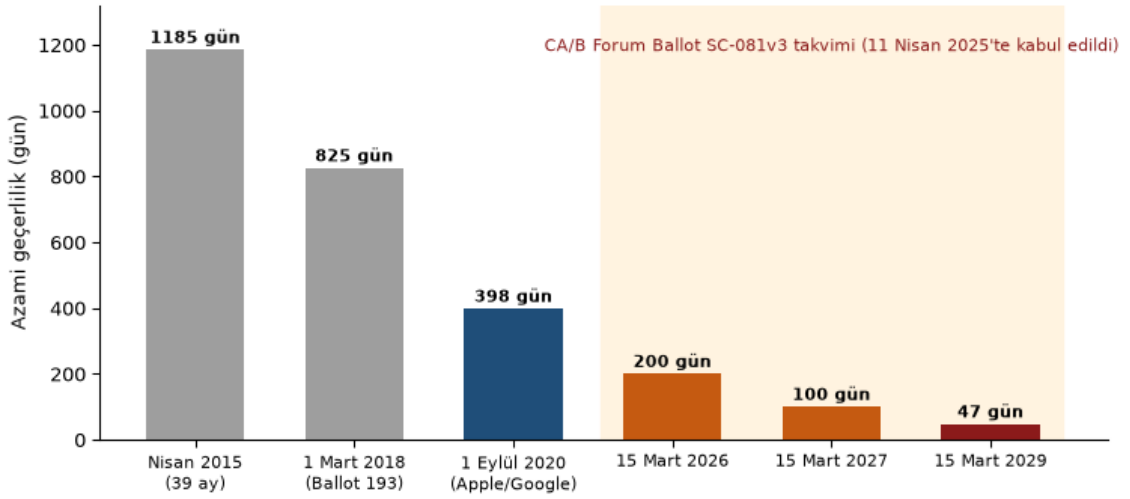
DigiNotar sonrasında geliştirilen **Sertifika Şeffaflığı (Certificate Transparency, CT)**, CA'ları engellemek yerine görünür kılmayı hedefler. Her sertifika, herkesin okuyabildiği ve yalnızca eklenebilen, Merkle ağacı yapısındaki kayıt defterlerine yazılır; defter bir kayıt makbuzu (Signed Certificate Timestamp, SCT) döndürür (Laurie vd., 2013; Laurie vd., 2021). Chrome, 30 Nisan 2018'den sonra düzenlenen sertifikalar için CT kaydını zorunlu tutmaktadır (Google Chrome, tarihsiz). Böylece bir alan adı sahibi, kendi adına düzenlenen her sertifikayı crt.sh gibi arama araçlarıyla izleyebilir. Adli bilişim incelemelerinde de CT kayıtları, bir alan adının hangi tarihte hangi CA'dan sertifika aldığını gösteren bağımsız ve değiştirilemez bir kaynaktır.

Web'in şifreli hâle gelmesinde en büyük pay, 2015'te ilk sertifikasını veren ücretsiz ve otomatik CA **Let's Encrypt**'e aittir. Aas ve arkadaşlarının (2019) çalışmasına göre kuruluş Ocak 2019'a kadar 223 milyon alan adı için 538 milyonu aşkın sertifika düzenlemiş ve dünyanın en büyük HTTPS sertifika otoritesi olmuştu. Kuruluşun yayımladığı günlük istatistiklere göre 27 Eylül 2026 itibarıyla yaklaşık 692 milyon etkin sertifika ve 231 milyon etkin kayıtlı alan adı bulunmaktadır (Let's Encrypt, 2026). Let's Encrypt, gizlilik gerekçesiyle OCSP hizmetini 6 Ağustos 2025'te tamamen kapatmış ve iptal bilgisini yalnızca CRL üzerinden yayımlamaya başlamıştır (Let's Encrypt, 2025).

2.4. Kısalan Sertifika Ömrü

Sertifika süreleri son on yılda sürekli kısalmıştır. 2015'te 39 ay olan üst sınır Mart 2018'de 825 güne, Eylül 2020'de 398 güne inmiştir (Sectigo, tarihsiz). CA/Browser Forum'un 11 Nisan 2025'te kabul ettiği SC-081v3 kararı, bu süreyi 15 Mart 2026'dan itibaren 200 güne, 15 Mart 2027'den itibaren 100 güne ve 15 Mart 2029'dan itibaren 47 güne düşürmektedir (CA/Browser Forum, 2025). Şekil 2 bu gelişimi göstermektedir. Kısa ömrün mantığı basittir: iptal mekanizmaları pratikte güvenilir çalışmadığından, çalınan bir anahtarın zarar verebileceği süre sertifikanın ömrüyle sınırlanır. Uygulamadaki sonucu ise sertifika yenilemenin artık elle yapılamayacağıdır. ACME protokolüyle otomatik yenileme yapmayan kurumlar 2027'den itibaren yılda en az dört kez, 2029'dan itibaren yaklaşık sekiz kez sertifika değiştirmek zorunda kalacaktır. Bu otomasyon, ileride sertifika imzalarının kuantum sonrası algoritmalara taşınmasını da kolaylaştıracaktır.

buraklogin.com



Kaynak: CA/Browser Forum (2025) ve Sectigo (tarihsiz) temel alınarak derlenmiştir. Gri ve mavi çubuklar geçmiş üst sınırlardır.

Şekil 2. Genel güvenilen TLS sertifikalarının azami geçerlilik süresinin gelişimi

2.5. Parolasız Kimlik Doğrulama: WebAuthn ve Geçiş Anahtarları

Açık anahtarlı kriptografinin son yıllarda en hızlı yayılan kullanımı, parolaların yerini alan **geçiş anahtarlarıdır (passkeys)**. W3C'nin WebAuthn standardında kullanıcı her site için cihazında ayrı bir anahtar çifti üretir; site yalnızca açık anahtarı saklar ve oturum açılırken cihaz, sitenin gönderdiği rastgele bir meydan okumayı özel anahtarla imzalar. Standart, COSE tanımlayıcılarıyla ECDSA P-256 (ES256), EdDSA ve RSA imzalarını destekler; belgedeki örnekler ES256'yı öne çıkarır (W3C, 2021). WebAuthn Seviye 3, 25 Ağustos 2026'da W3C Tavsiyesi olarak yayımlanmıştır (W3C, 2026). İmza alan adına bağlı olduğu için sahte bir sitede üretilen imza gerçek sitede işe yaramaz; bu da oltalama saldırılarını yapısal olarak etkisiz kılar. FIDO Alliance, Mayıs 2026'da dünyada 5 milyar geçiş anahtarının kullanımda olduğunu açıklamıştır (FIDO Alliance, 2026).

3. Algoritmaların Protokollerde Birleşimi

Tek bir algoritma nadiren tek başına kullanılır. Kullanıcıların gerçekte karşılaştığı şey, yukarıdaki ilkellerin belirli bir sırayla birleştirildiği protokollerdir. Bu bölüm en yaygın protokolleri, hangi algoritmayı nerede kullandıklarına odaklanarak incelemektedir.

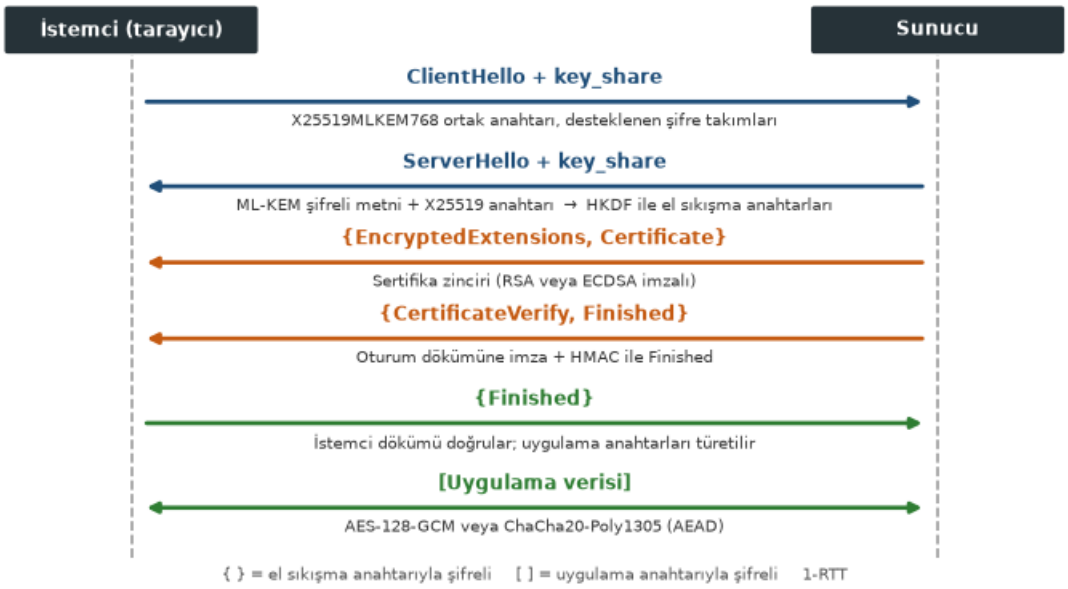
3.1. TLS 1.3

Web trafiğini koruyan **TLS (Transport Layer Security)** protokolünün 2018'de yayımlanan 1.3 sürümü, önceki sürümlerin biriktirdiği sorunlu seçenekleri temizlemiştir (Rescorla, 2018). RSA ile anahtar taşıma, statik DH, CBC kipi, RC4, SHA-1 ve MD5 protokolden çıkarılmıştır. Geriye kalan şifre takımları yalnızca AEAD kiplerinden oluşur: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384 ve TLS_CHACHA20_POLY1305_SHA256. Anahtar değişimi her zaman geçici (EC)DH ile yapıldığı için ileri gizlilik zorunludur. El sıkışma, önceki sürümlerin iki gidiş-dönüşü yerine tek gidiş-dönüşte (1-RTT) tamamlanır ve sunucu sertifikası da şifreli olarak iletilir.

Şekil 3, güncel bir tarayıcı ile sunucu arasındaki TLS 1.3 el sıkışmasını adım adım göstermektedir. Chrome 131 (Kasım 2024) ve Firefox 132'den (Ekim 2024; Mozilla, 2024)

burakolgun.com

itibaren istemcinin ilk mesajı klasik X25519 ile kuantum sonrası ML-KEM-768'i birleştiren **X25519MLKEM768** hibrit anahtarını taşır. Sunucu bu grubu destekliyorsa her iki yöntemin sırları birleştirilerek HKDF'ye verilir; biri kırılsa bile diğeri oturumu korumaya devam eder. Sertifika imzası ise hâlâ klasik RSA veya ECDSA'dır. Bu asimetrinin nedeni Kısım 5.3'te açıklanmaktadır.



Kaynak: RFC 8446 (Rescorla, 2018) ve IETF hibrit anahtar değişimi taslağı temel alınarak derlenmiştir.

Şekil 3. Hibrit anahtar değişimli TLS 1.3 el sıkışmasında kullanılan algoritmalar

3.2. SSH, Signal ve Wi-Fi

SSH protokolünün en yaygın uygulaması OpenSSH, 2022'de 9.0 sürümüyle NTRU Prime ve X25519'u birleştiren hibrit anahtar değişimini varsayılan yaptı; Nisan 2025'te çıkan 10.0 sürümünde varsayılan yöntem mlkem768x25519-sha256 oldu (OpenSSH, 2025). Kullanıcı kimlik doğrulamasında Ed25519 anahtarları, RSA'nın yerini büyük ölçüde almıştır.

Signal protokolü, WhatsApp, Signal ve Facebook Messenger dahil olmak üzere milyarlarca kullanıcının uçtan uca şifrelemesinin temelidir. Protokol iki parçadan oluşur: oturum başlatan X3DH (sonraki sürümünde PQXDH) anahtar anlaşması ve her mesajda anahtarları yenileyen **Double Ratchet** algoritması. Double Ratchet, her mesaj için yeni bir anahtar türetir; bir anahtarın ele geçirilmesi ne önceki ne de sonraki mesajları açığa çıkarır (Marlinspike ve Perrin, 2016). Signal 2023'te X25519 ile Kyber'i birleştiren PQXDH'yi devreye aldı; Apple da 2024'te iMessage için benzer yapıdaki PQ3 protokolünü duyurdu.

WPA3 kablosuz ağ güvenliği, WPA2'nin önceden paylaşılan anahtar yönteminin çevrimdışı sözlük saldırısına açık olması sorununu Dragonfly tabanlı **SAE (Simultaneous Authentication of Equals)** el sıkışmasıyla çözer. Vanhoef ve Ronen (2020), ilk uygulamalarda zamanlama ve önbellek yan kanalları yoluyla parolanın sızdırılabildiğini "Dragonblood" adıyla gösterdi; standart buna göre güncellendi.

3.3. Disk Şifreleme, Elektronik İmza ve Blokzincir

BitLocker, FileVault ve Linux LUKS gibi tam disk şifreleme çözümleri AES-XTS kullanır. Anahtar genellikle TPM ya da Secure Enclave gibi bir donanım modülünde saklanır ve kullanıcı parolası Argon2 veya PBKDF2 ile türetilen bir anahtarla birleştirilir. Adli incelemede sabit diskin kendisi değil, bu anahtar zincirinin ele geçirilip geçirilemeyeceği belirleyicidir.

Türkiye'de nitelikli elektronik sertifikalar ve UYAP'ta kullanılan e-imzalar, akıllı kart içindeki RSA veya ECDSA özel anahtarlarıyla, SHA-256 özetleri üzerinden üretilir. Özel anahtar kartın dışına çıkmaz; imza işlemi kartın içindeki güvenli işlemcide yapılır. Bitcoin ise secp256k1 üzerinde ECDSA ve 2021'deki Taproot güncellemesiyle eklenen Schnorr imzaları ile SHA-256 ve RIPEMD-160 özetlerini kullanır. Tablo 1, yaygın uygulamalarda kullanılan algoritma bileşimlerini özetlemektedir.

Tablo 1. Yaygın uygulamalarda kullanılan kriptografik algoritma bileşimleri

Uygulama	Anahtar anlaşması	Kimlik doğrulama	Veri şifreleme	Özet / KDF
TLS 1.3 (web)	X25519MLKEM768, X25519	RSA-PSS, ECDSA P-256	AES-GCM, ChaCha20-Poly1305	SHA-256/384, HKDF
OpenSSH 10	mlkem768x25519	Ed25519, ECDSA, RSA	ChaCha20-Poly1305, AES-GCM	SHA-256/512
Signal / WhatsApp	X3DH / PQXDH (X25519+Kyber)	Ed25519 / XEdDSA	AES-256-CBC + HMAC	HKDF-SHA256
WireGuard	X25519 (Noise IK)	Statik X25519 anahtarı	ChaCha20-Poly1305	BLAKE2s, HKDF
WPA3-Personal	SAE (Dragonfly)	Parola tabanlı	AES-CCMP/GCMP	SHA-256
BitLocker / LUKS2	-	TPM + PIN / parola	AES-XTS	PBKDF2 / Argon2id
Türkiye e-imza	-	RSA-2048 veya ECDSA	-	SHA-256
Bitcoin	-	ECDSA / Schnorr (secp256k1)	-	SHA-256, RIPEMD-160

Not. Kaynak: Rescorla (2018), OpenSSH (2025), Marlinspike ve Perrin (2016), Donenfeld (2017) ve Kamu SM belgeleri temel alınarak derlenmiştir.

4. Rastgelelik ve Anahtar Yönetimi

4.1. Kriptografik Rastgele Sayı Üretimi

Bu makalede incelenen algoritmaların neredeyse tamamı bir noktada rastgele sayıya ihtiyaç duyar: AES anahtarı, GCM nonce'u, RSA'nın asal sayıları, ECDSA'nın k değeri ve TLS'in geçici DH anahtarları. Rastgelelik zayıfsa algoritmanın gücü önemini yitirir. NIST bu alanı üç belgeyle düzenler. SP 800-90B, fiziksel gürültü kaynaklarından (saat titremesi, termal gürültü, kullanıcı etkileşimi) elde edilen entropinin nasıl ölçüleceğini ve test edileceğini tanımlar (Sönmez Turan vd., 2018). SP 800-90A Rev. 1, bu entropiyi tohum olarak kullanıp uzun sözde rastgele diziler üreten deterministik üreteçleri (Hash_DRBG, HMAC_DRBG, CTR_DRBG) belirler (Barker ve Kelsey, 2015). Eylül 2025'te nihai hâline getirilen SP 800-90C ise bu iki parçanın bir araya getirilmesini dört üreteç sınıfı üzerinden tarif eder (Barker vd., 2025).

Zayıf rastgeleliğin gerçek dünyadaki boyutunu 2012'de birbirinden bağımsız iki ekip ölçtü. Heninger ve arkadaşları (2012) İnternet'in tamamını tarayarak, TLS sunucularının

%0,50'sinin ve SSH sunucularının %0,03'ünün RSA özel anahtarını, SSH sunucularının %1,03'ünün ise DSA özel anahtarını hesaplayabildiklerini gösterdi. Hesaplama için karmaşık bir yönteme gerek yoktu: aynı asal çarpanı paylaşan iki RSA modülünün en büyük ortak böleni alınınca her iki anahtar da çarpanlarına ayrılıyordu. Sorunlu cihazların büyük kısmı, açılışta yeterli entropi toplayamadan anahtar üreten yönlendirici ve güvenlik duvarı gibi gömülü cihazlardı. Lenstra ve arkadaşları (2012) aynı dönemde topladıkları açık anahtarlarda, her bin RSA modülünden ikisinin hiçbir güvenlik sağlamadığını bildirdi. Serinin birinci bölümünde ele alınan Debian OpenSSL ve Dual_EC_DRBG olayları da aynı sorunun farklı yüzleridir.

Pratik kural açıktır: uygulama geliştiriciler kendi rastgele sayı üreteçlerini yazmamalı, Python'da random yerine secrets veya os.urandom, Java'da SecureRandom, Windows'ta BCryptGenRandom, Linux'ta getrandom çağrısı gibi işletim sisteminin kriptografik üretecini kullanmalıdır. Gömülü cihaz üreticileri ise anahtarları ilk açılışta değil, yeterli entropi toplandıktan sonra üretmelidir.

4.2. Anahtar Yaşam Döngüsü

Kriptografik sistemlerin büyük kısmı, algoritma kırıldığı için değil, anahtar kötü yönetildiği için tehlikeye girer. NIST SP 800-57, bir anahtarın yaşam döngüsünü üretim, dağıtım, kullanım, yedekleme, arşivleme, iptal ve imha aşamalarıyla tanımlar ve her anahtar türü için bir **kriptoperiyot**, yani kullanım süresi üst sınırı önerir (Barker, 2020). Temel ilkeler şunlardır:

- **Tek amaç:** Aynı anahtar hem şifreleme hem imza için kullanılmamalıdır. RSA'da bu ayrım yapılmadığında bir işlemin çıktısı diğerine karşı saldırıda kullanılabilir.
- **Ayrı saklama:** Şifreli veri ile onu çözen anahtar aynı ortamda tutulmamalıdır. KVKK Kurulu'nun özel nitelikli veriler için aradığı "anahtarların güvenli ve farklı ortamlarda tutulması" şartı bu ilkenin hukuki karşılığıdır (KVKK, 2018b).
- **Periyodik yenileme:** Uzun ömürlü anahtarlar belirli aralıklarla yenilenmeli; sızıntı şüphesinde derhal iptal edilmelidir. Kısalan sertifika ömürleri (Kısım 2.4) bu ilkeyi web ölçeğinde zorunlu kılmaktadır.
- **Yedekleme ve paylaştırma:** Kritik anahtarlar tek bir kişinin elinde bulunmamalıdır. Shamir'in (1979) gizli paylaştırma yöntemi, bir anahtarı n parçaya bölüp herhangi k parçayla yeniden oluşturulmasına, k-1 parçanın ise hiçbir bilgi vermemesine izin verir. Kök CA anahtarlarının ve kripto para soğuk cüzdanlarının yedeklenmesinde yaygın olarak kullanılır.

4.3. Donanım Güvenlik Modülleri ve FIPS 140-3

Yüksek değerli anahtarlar yazılımda değil, **donanım güvenlik modüllerinde (Hardware Security Module, HSM)** saklanır. HSM, anahtarı dışarı vermeden imzalama ve şifreleme işlemini kendi içinde yapan, fiziksel müdahaleyi algıladığında anahtarları silen özel bir cihazdır. Kök sertifika otoriteleri, bankaların kart doğrulama sistemleri ve e-imza altyapıları HSM kullanır. Kişisel bilgisayarlardaki karşılığı, ISO/IEC 11889:2015 olarak standartlaşmış **Güvenilir Platform Modülü (TPM 2.0)**'dır (ISO/IEC, 2015); Windows 11'in TPM 2.0 şartı

burakdgn.com

ve BitLocker'ın disk anahtarını TPM'de mühürlemesi bu standarda dayanır. Akıllı kartlı e-imzalar da aynı ilkeyle çalışır: özel anahtar kartın içinde üretilir ve karttan hiç çıkmaz.

Kriptografik modüllerin güvenliği ABD ve Kanada'nın ortak yürüttüğü Kriptografik Modül Doğrulama Programı (CMVP) kapsamında FIPS 140 standardına göre sertifikalandırılır. 22 Eylül 2019'da yürürlüğe giren FIPS 140-3, önceki sürümün yerini almıştır (NIST, 2019). Geçiş sürecinin son adımı olarak 22 Eylül 2026 itibarıyla tüm FIPS 140-2 sertifikaları "tarihsel liste"ye taşınmıştır; bu modüllerin yeni alımlarda kullanılması önerilmemektedir (NIST, tarihsiz). Kamu ihalelerinde "FIPS 140-2 sertifikalı" ifadesi geçen teknik şartnamelerin bu tarihten sonra güncellenmesi gerekir.

5. Kuantum Tehdidi ve Kuantum Sonrası Kriptografi

5.1. Shor ve Grover Algoritmaları

Peter Shor 1994'te, yeterince büyük bir kuantum bilgisayarın çarpanlara ayırma ve ayrık logaritma problemlerini polinom zamanda çözebileceğini gösterdi (Shor, 1994). Bu sonuç RSA, DH, ECDH ve ECDSA'nın tamamını etkiler; anahtar uzunluğunu artırmak çözüm değildir. Gereken kaynak tahminleri ise hızla düşmektedir. Gidney ve Ekerå (2021) 2048 bitlik bir RSA anahtarının yaklaşık 20 milyon gürültülü kübitle sekiz saatte çarpanlarına ayrılabileceğini hesaplamıştı; Gidney (2025) aynı işin bir milyondan az gürültülü kübitle bir haftadan kısa sürede yapılabileceğini gösterdi. Bugünkü kuantum işlemciler hâlâ bu ölçeğin çok gerisindedir, ancak gereken kaynağın her yeni çalışmada küçüldüğü açıktır.

Lov Grover'ın (1996) arama algoritması ise simetrik anahtarlara karşı karekök düzeyinde bir hızlanma sağlar; 128 bitlik bir anahtarın aranması teorik olarak 2^64 kuantum işlemine iner. Ne var ki Grover'ın adımları paralelleştirilemez ve her adım hata düzeltmeli kübitlerle yürütülmelidir. Bu nedenle pratik maliyeti çok yüksektir ve AES-256'ya geçiş ihtiyatlı bir önlem olarak görülür, acil bir zorunluluk olarak değil. SHA-256 ve SHA-3 de benzer biçimde yeterli kabul edilmektedir.

Tehdidin bugünden ciddiye alınmasının nedeni **"şimdi topla, sonra çöz" (harvest now, decrypt later)** senaryosudur. Bugün şifreli olarak kaydedilen trafik, 10-15 yıl sonra kuantum bilgisayar kullanılabilir olduğunda çözülebilir. Sağlık kayıtları, devlet sırları, ticari sırlar ve kişisel veriler gibi uzun süre gizli kalması gereken bilgiler için risk bugünden başlamaktadır. Mosca'nın (2018) formülasyonuyla, verinin gizli kalması gereken süre ile geçişin tamamlanması için gereken sürenin toplamı, kuantum bilgisayarın gelmesine kalan süreden uzunsa kurum zaten geç kalmıştır.

5.2. NIST Standartları

NIST 2016'da başlattığı yarışmaya 69 geçerli başvuru aldı. Birkaç eleme turu sırasında bazı güçlü adaylar klasik bilgisayarlarla kırıldı; örneğin izojeni tabanlı SIKE, 2022'de tek bir dizüstü bilgisayarla bir saatten kısa sürede çözüldü (Castryck ve Decru, 2023). Bu olay, yeni algoritmalara temkinli yaklaşmanın ve hibrit kullanımın neden önemli olduğunu gösterdi. Ağustos 2024'te üç standart yayımlandı:

burakgun.com

- **FIPS 203, ML-KEM** (eski adıyla CRYSTALS-Kyber): Modül kafes üzerinde hatalı öğrenme (Module Learning With Errors, MLWE) problemine dayanan anahtar kapsülleme mekanizması. Anahtar değişimi için birincil standarttır (NIST, 2024a).
- **FIPS 204, ML-DSA** (CRYSTALS-Dilithium): Yine modül kafes tabanlı, genel amaçlı dijital imza standardı (NIST, 2024b).
- **FIPS 205, SLH-DSA** (SPHINCS+): Yalnızca özet fonksiyonlarının güvenliğine dayanan durumsuz imza şeması. Kafes problemlerinde beklenmedik bir kırılmaya karşı yedektir; imzaları büyük ve yavaştır (NIST, 2024c).

FALCON tabanlı **FN-DSA** (taslak FIPS 206) kısa imzası sayesinde bant genişliği kısıtlı senaryolar için hazırlanmaktadır. NIST Mart 2025'te ise kod tabanlı **HQC** algoritmasını ML-KEM'e matematiksel olarak farklı bir yedek olarak seçmiştir (NIST, 2025). Tablo 2 bu standartları özetlemektedir.

Tablo 2. NIST kuantum sonrası kriptografi standartları (Eylül 2026 itibarıyla)

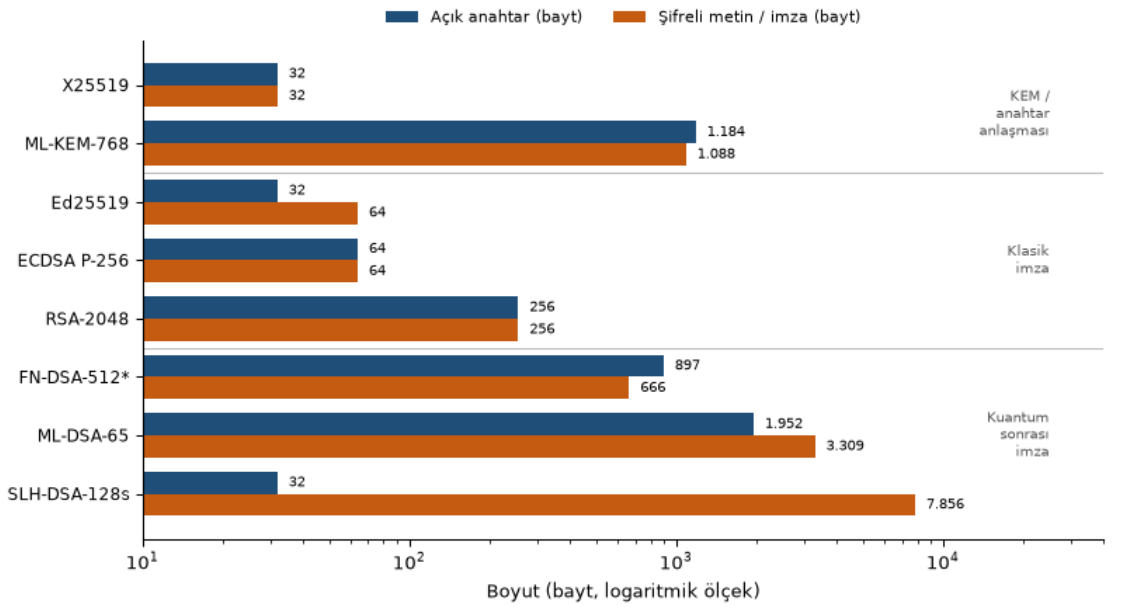
Standart	Algoritma (eski ad)	Tür	Matematiksel temel	Durum
FIPS 203	ML-KEM (Kyber)	Anahtar kapsülleme	Modül kafes (MLWE)	Yayımlandı (08/2024)
FIPS 204	ML-DSA (Dilithium)	Dijital imza	Modül kafes (MLWE/MSIS)	Yayımlandı (08/2024)
FIPS 205	SLH-DSA (SPHINCS+)	Dijital imza	Özet fonksiyonları	Yayımlandı (08/2024)
FIPS 206	FN-DSA (FALCON)	Dijital imza	NTRU kafesi	Taslak
-	HQC	Anahtar kapsülleme	Kodlama teorisi	Seçildi (03/2025), taslak bekleniyor

Not. Kaynak: NIST (2024a, 2024b, 2024c, 2025) ve Moody vd. (2024) temel alınarak derlenmiştir.

5.3. Geçişin Pratik Güçlükleri

Kuantum sonrası algoritmaların en görünür bedeli boyuttur. Şekil 4'te görüldüğü gibi X25519 açık anahtarı 32 bayt iken ML-KEM-768'in açık anahtarı 1.184, şifreli metni 1.088 bayttır. İmzalarda fark daha büyüktür: 64 baytlık bir Ed25519 imzasının yerini 3.309 baytlık bir ML-DSA-65 imzası alır. Bir TLS sertifika zincirinde birkaç imza ve açık anahtar bulunduğu için, imzaların tamamen kuantum sonrasına taşınması el sıkışmayı onlarca kilobayt büyütebilir. Bu, anahtar değişiminin 2024-2025'te hızla geçmesine karşın sertifika imzalarının hâlâ klasik kalmasının temel nedenidir. Anahtar değişiminin öncelikli olması mantıklıdır: "şimdi topla, sonra çöz" saldırısı yalnızca gizliliği tehdit eder; imzanın taklit edilmesi ise saldırı anında kuantum bilgisayar gerektirir.

burakozturk.com



*Kaynak: FIPS 203, 204, 205 (NIST, 2024a-c), RFC 7748, RFC 8032 temel alınarak derlenmiştir. *FN-DSA taslak, imza ortalama boyut.*

Şekil 4. Klasik ve kuantum sonrası algoritmalarda açık anahtar ile şifreli metin/imza boyutları

Boyut sorununun pratik bir yansıması da vardır. Hibrit anahtar değişiminin ilk denemelerinde bazı eski güvenlik duvarları ve yük dengeleyiciler, tek bir TCP paketine sığmayan büyük ClientHello mesajlarını hatalı işleyerek bağlantıları kesmiştir. Chrome 124 ile Nisan 2024'te hibrit anahtar değişimi varsayılan hâle geldiğinde, 1.500 baytı aşıp birden fazla pakete bölünen ClientHello mesajlarını okuyamayan kurumsal güvenlik cihazları nedeniyle bağlantı sorunları raporlanmıştır (tldr.fail, tarihsiz; Chromium, 2024). Bu tür sorunlar kuantum sonrası geçişin yalnızca kriptografik değil, aynı zamanda ağ altyapısı sorunu olduğunu göstermektedir.

5.4. Ulusal Geçiş Takvimleri

Geçiş takvimleri 2024-2025 arasında büyük ölçüde netleşmiştir. NIST'in Kasım 2024'te taslak olarak yayımladığı IR 8547, 112 bitlik güvenlik sağlayan kuantuma açık algoritmaların (RSA-2048, P-224 vb.) 2030'dan sonra kullanımdan kaldırılmasını (deprecated), 2035'ten sonra ise tüm kuantuma açık algoritmaların tamamen yasaklanmasını (disallowed) öngörmektedir (Moody vd., 2024). Birleşik Krallık Ulusal Siber Güvenlik Merkezi (NCSC), Mart 2025'te kurumların 2028'e kadar envanter ve plan çıkarmasını, en öncelikli sistemleri 2031'e kadar taşımasını ve geçişi 2035'e kadar tamamlamasını istemiştir (NCSC, 2025). Avrupa Birliği'nin NIS İşbirliği Grubu ise 23 Haziran 2025'te yayımladığı koordineli yol haritasında üye devletlerden 2026 sonuna kadar ulusal planlarını hazırlamalarını, yüksek riskli kullanım alanlarını 2030 sonuna kadar taşımalarını ve kalan sistemleri mümkün olduğunca 2035'e kadar dönüştürmelerini beklemektedir (NIS Cooperation Group, 2025). Tablo 3 bu takvimleri karşılaştırmaktadır.

Özel sektörde geçiş, düzenleyicilerin önüne geçmiştir. Cloudflare, Ekim 2025'te ağından geçen insan kaynaklı trafiğin yarısından fazlasının kuantum sonrası anahtar değişimiyle korunduğunu bildirmiş (Westerbaan, 2025), Nisan 2026'da bu oranın %65'i aştığını ve imzalar dahil tam kuantum sonrası güvenliğe 2029'da ulaşmayı hedeflediğini

açıklamıştır (Westerbaan, 2026). Türkiye için benzer bir ulusal takvim henüz ilan edilmemiştir; konu Kısım 8'de ele alınmaktadır.

Tablo 3. Kuantum sonrası kriptografiye geçiş takvimlerinin karşılaştırılması

Kurum / ülke	Belge	Ara hedef	Öncelikli sistemler	Tam geçiş
NIST (ABD)	IR 8547 (taslak, 2024)	112 bit algoritmalar 2030 sonrası kaldırılır	-	2035 sonrası kuantuma açık algoritmalar yasak
NCSC (Birleşik Krallık)	PQC migration timelines (2025)	2028: envanter ve plan	2031	2035
AB (NIS İşbirliği Grubu)	Koordineli yol haritası (2025)	2026 sonu: ulusal planlar	2030 sonu (yüksek risk)	2035 (mümkün olduğunca)
Cloudflare (sektör)	Yol haritası (2026)	Anahtar değişimi: trafiğin %65+	-	2029 (imzalar dahil)
Türkiye	-	İlan edilmiş takvim yok	-	-

Not. Kaynak: Moody vd. (2024), NCSC (2025), NIS Cooperation Group (2025), Westerbaan (2025) ve Westerbaan (2026) temel alınarak derlenmiştir.

5.5. Durumlu Özet Tabanlı İmzalar

Kuantum sonrası imzaların en eski ve en iyi anlaşılmış ailesi, güvenliği yalnızca özet fonksiyonlarına dayanan Merkle ağacı tabanlı şemalardır. **XMSS** (RFC 8391) ve **LMS** (RFC 8554), NIST tarafından Ekim 2020'de SP 800-208 ile onaylanmıştır (Huelsing vd., 2018; McGrew vd., 2019; Cooper vd., 2020). Bu şemalar "durumlu"dur: her tek kullanımlık anahtar yalnızca bir kez kullanılabilir ve imzalayan tarafın hangi anahtarları kullandığını hatasız kaydetmesi gerekir. Bir anahtarın iki kez kullanılması, örneğin bir HSM yedeğinden geri dönülmesi hâlinde güvenlik çöker. Bu kırılganlık nedeniyle XMSS ve LMS genel kullanım için değil, imza sayısının sınırlı ve imzalayan ortamın sıkı denetlendiği yazılım ve donanım yazılımı (firmware) imzalama gibi senaryolar için önerilmektedir. Durumsuz SLH-DSA (FIPS 205) bu sorunu ortadan kaldırır, ancak serinin birinci bölümündeki ölçümlerde görüldüğü gibi çok daha yavaştır.

6. İleri Kriptografik Yapılar

Klasik kriptografi veriyi saklarken ve taşırken korur; işlenirken ise verinin açılması gerekir. Son yirmi yılda olgunlaşan bir grup yapı, veriyi açmadan üzerinde işlem yapmayı veya bilgiyi açıklamadan bir iddiayı kanıtlamayı mümkün kılmaktadır. Bu yapılar henüz AES veya RSA kadar yaygın değildir, ancak üretim sistemlerine girmeye başlamışlardır. Tablo 4 bu yapıları özetlemektedir.

6.1. Sıfır Bilgi İspatları

Sıfır bilgi ispatı (zero-knowledge proof), bir tarafın bir ifadenin doğru olduğunu, ifadenin doğruluğu dışında hiçbir bilgi vermeden kanıtlamasıdır. Örneğin bir kullanıcı doğum tarihini açıklamadan 18 yaşından büyük olduğunu ya da parolasını göndermeden onu bildiğini kanıtlayabilir. Kavram, Goldwasser, Micali ve Rackoff'un (1989) etkileşimli ispat sistemleri üzerine çalışmasıyla tanımlanmıştır. Uygulamadaki en yaygın biçimi, kısa ve hızlı doğrulanan etkileşimsiz ispatlar üreten **zk-SNARK**'lardır. Groth'un (2016) önerdiği yapı, ispatı yalnızca üç grup elemanından oluşacak kadar küçültmüştür.

burakolgun.com

Zcash kripto parası, gönderen, alıcı ve miktarı gizleyen korumalı işlemlerde zk-SNARK kullanır; Ekim 2018'deki Sapling güncellemesiyle Groth16 yapısına geçmiştir. Aynı proje, ileri kriptografinin risklerine de örnek oluşturur. Önceki BCTV14 ispat sistemindeki bir hata, fark edilmeden sahte para basılmasına izin verebilecek nitelikteydi; hata Mart 2018'de bulunmuş, gizlice giderilmiş ve Şubat 2019'da kamuoyuna açıklanmıştır (Swihart, 2019). Karmaşık yapılarda tek bir hatanın sonuçları, kullanılan matematiğin olgunluğuyla orantılı olarak ağırlaşabilmektedir.

6.2. Homomorfik Şifreleme

Tam homomorfik şifreleme (Fully Homomorphic Encryption, FHE), şifreli veriler üzerinde toplama ve çarpma işlemlerinin, veriyi hiç çözmeden yapılabilmesidir. Sonuç çözüldüğünde, işlem açık veri üzerinde yapılmış gibi doğru cevap elde edilir. RSA'nın 1978'deki yayımından beri tartışılan bu fikrin ilk tam çözümünü Craig Gentry 2009'da ideal kafesler üzerinde vermiştir (Gentry, 2009). İlk şemalar pratik olamayacak kadar yavaştı; bugün hâlâ açık veri üzerindeki işleme göre birkaç büyüklük mertebesi yavaş olsalar da sınırlı görevlerde üretime girmişlerdir.

Apple, Temmuz 2024'te açık kaynak olarak yayımladığı Swift Homomorphic Encryption kütüphanesinin iOS 18'deki arayan kimliği sorgulama özelliğinde kullanıldığını açıklamıştır. Telefon, gelen aramanın numarasını şifreli olarak sunucuya gönderir; sunucu numarayı hiç görmeden şifreli veritabanında arama yapar ve şifreli sonucu döndürür. Kullanılan BFV şeması kafes tabanlı olduğu için kuantum sonrası güvenlik de sağlar (Boemer vd., 2024). Kişisel verilerin bulutta işlenmesi konusunda KVKK ve GDPR'ın getirdiği kısıtlar düşünüldüğünde, bu tür yapıların sağlık ve finans sektörlerinde önem kazanması beklenmektedir.

6.3. Güvenli Çok Taraflı Hesaplama ve Gizli Paylaştırma

Güvenli çok taraflı hesaplama (Secure Multi-Party Computation, MPC), birden fazla tarafın kendi girdilerini birbirine göstermeden ortak bir fonksiyonu hesaplamasını sağlar. Andrew Yao'nun (1982) iki milyonerin hangisinin daha zengin olduğunu servetlerini açıklamadan bulması problemiyle başlattığı alan, bugün bankaların dolandırıcılık verilerini paylaşmadan ortak analiz yapmasından kripto para saklama hizmetlerinde özel anahtarın hiçbir zaman tek bir yerde bir araya getirilmemesine kadar geniş bir uygulama yelpazesine sahiptir. MPC'nin temel yapı taşlarından biri, Kısım 4.2'de anahtar yedekleme bağlamında değinilen Shamir'in (1979) gizli paylaştırma yöntemidir.

Tablo 4. İleri kriptografik yapılar ve örnek kullanımlar

Yapı	Sağladığı özellik	Temel çalışma	Örnek kullanım
Gizli paylaştırma	Sır n parçaya bölünür; k parça gerekir	Shamir (1979)	Kök CA ve soğuk cüzdan yedekleri
Güvenli çok taraflı hesaplama	Girdiler gizli kalarak ortak hesaplama	Yao (1982)	Eşik imzalı kripto saklama, ortak analiz
Sıfır bilgi ispatı	Bilgi vermeden doğruluğu kanıtlama	Goldwasser vd. (1989); Groth (2016)	Zcash korumalı işlemler
Tam homomorfik şifreleme	Şifreli veri üzerinde işlem	Gentry (2009)	Apple iOS 18 arayan kimliği sorgusu

burkologun.com

Not. Kaynak: Shamir (1979), Yao (1982), Goldwasser vd. (1989), Gentry (2009), Groth (2016), Swihart (2019) ve Boemer vd. (2024) temel alınarak derlenmiştir.

7. Şifreleme Politikası ve Yasal Erişim Tartışması

7.1. Anahtar Emaneti ve Clipper Çipi

Güçlü şifrelemenin yaygınlaşması, kolluk ve istihbarat kurumlarıyla teknoloji topluluğu arasında 1990'lardan beri süren bir tartışmayı beraberinde getirmiştir. Tartışmanın başlangıç noktası, ABD hükümetinin 16 Nisan 1993'te duyurduğu **Clipper çipi**dir. Çip, gizli tutulan Skipjack algoritmasıyla şifreleme yapıyor, ancak oturum anahtarını devletin emanetindeki bir anahtarla şifreleyip "kolluk erişim alanı" (LEAF) adı verilen bir veri bloğunda iletiyordu. Matt Blaze (1994), LEAF'i doğrulayan sağlama değerinin yalnızca 16 bit olduğunu, bu nedenle yaklaşık 2^16 denemeyle geçerli görünen sahte bir LEAF üretilip emanet mekanizmasının tamamen atlatılabileceğini gösterdi. Blaze'in ölçümüne göre bu işlem tek bir kartla yaklaşık 42 dakika sürüyordu. Clipper hiçbir zaman yaygınlaşmadı.

Aynı tartışma 2015'te yeniden alevlenince, aralarında Whitfield Diffie ve Ronald Rivest'in de bulunduğu 15 kriptograf ve güvenlik araştırmacısı "Keys Under Doormats" başlıklı çalışmayı yayımladı. Yazarlara göre kolluğa özel erişim sağlamak için tasarlanan her mekanizma, ileri gizlilik gibi modern güvenlik özelliklerini ortadan kaldırmakta, sistem karmaşıklığını artırmakta ve tek bir yüksek değerli hedef yaratmaktadır (Abelson vd., 2015). Serinin birinci bölümünde anlatılan Dual_EC_DRBG ve Juniper olayı, bu uyarının teorik olmadığını göstermiştir: bir tarafa ayrılmış arka kapı, başka bir tarafın eline geçebilmektedir.

7.2. Güncel Tartışmalar

Tartışmanın en bilinen örneği, 2016'da San Bernardino saldırısıyla ilgili bir iPhone üzerinde yaşanmıştır. ABD mahkemesi 16 Şubat 2016'da Apple'a cihazın parola denemesi sınırlarını kaldıran özel bir yazılım üretmesini emretti; Apple aynı gün müşterilerine yazdığı açık mektupla buna itiraz etti (Apple, 2016). Hükümet 28 Mart 2016'da cihazın açıldığını bildirerek davadan çekildi. Birleşik Krallık'ta ise Investigatory Powers Act 2016 kapsamında Apple'a gönderilen teknik yeterlilik bildiriminin ardından Apple, 21 Şubat 2025'ten itibaren İngiltere'deki yeni kullanıcıların iCloud için uçtan uca şifreleme sağlayan Gelişmiş Veri Koruması özelliğini açmasını engelledi. iMessage ve FaceTime uçtan uca şifreli kalmaya devam etmektedir (Apple, 2025).

Avrupa Birliği'nde çevrim içi çocuk istismarıyla mücadele tüzüğü teklifi, kamuoyunda "sohbet denetimi" (chat control) adıyla bilinen tartışmanın merkezindedir. Teklifin şifreli mesajlaşma servislerinde içerik taramasını zorunlu kılabilecek hükümleri, uçtan uca şifrelemenin fiilen istemci tarafında delinmesi anlamına geleceği gerekçesiyle eleştirilmiştir. Konsey 26 Kasım 2025'te tutumunu belirlemiş (Council of the European Union, 2025), üçlü müzakereler Aralık 2025'te başlamış, ancak Haziran 2026'daki son turda uzlaşı sağlanamamıştır (European Parliament, 2026). Tartışmanın sonucu, Avrupa'da hizmet veren ve Türk kullanıcıların da yoğun olarak kullandığı mesajlaşma uygulamalarının şifreleme mimarisini doğrudan etkileyecektir.

burakolgun.com

Bu tartışmaların kriptografi açısından özü değişmemiştir: matematik, yalnızca "iyi niyetli" tarafların kullanabileceği bir zayıflık tanımlamaya izin vermez. Kolluğun meşru ihtiyaçları, uç cihazlara hukuki izinle erişim, üst veri analizi ve Kısım 8.3'te ele alınan el koyma yetkileri gibi şifrelemeyi zayıflatmayan yollarla karşılanmaya çalışılmaktadır.

8. Hukuki Çerçeve ve Türkiye Bağlamı

8.1. Elektronik İmza

23 Ocak 2004 tarihli ve 5070 sayılı **Elektronik İmza Kanunu**, güvenli elektronik imzanın elle atılan imzayla aynı hukuki sonucu doğurduğunu hükme bağlamıştır (m. 5). Kanunun teknik ayrıntısı, dönemin Telekomünikasyon Kurumu (bugünkü Bilgi Teknolojileri ve İletişim Kurumu) tarafından 6 Ocak 2005 tarihli ve 25692 sayılı Resmî Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ile düzenlenmiştir. Tebliğ, imza oluşturma ve doğrulama verileri ile özet algoritmalarının ETSI TS 102 176-1 standardına uygun olmasını şart koşmaktadır (Telekomünikasyon Kurumu, 2005). Bu atıf, algoritma listesinin Avrupa standardı güncellendikçe dolaylı olarak güncellenmesini sağlar. Kamu kurumlarına sertifika hizmeti veren **Kamu Sertifikasyon Merkezi (Kamu SM)** TÜBİTAK BİLGEM bünyesinde faaliyet göstermektedir. Kuantum sonrası imza algoritmalarının bu mevzuata ne zaman ve hangi yolla gireceği henüz belirlenmemiştir; ETSI ve Avrupa düzeyindeki gelişmeler belirleyici olacaktır.

Kısım 2.2'de anlatılan TÜRKTRUST olayı, e-imza ve SSL sertifika hizmeti veren yerli sağlayıcıların küresel tarayıcı güven depolarındaki konumunun ne kadar hassas olduğunu göstermiştir. Tarayıcı üreticilerinin kök sertifika programları, Türk hukukundaki yetkilendirmeden bağımsız teknik ve denetim şartları uygular; bir yerli sertifika otoritesinin bu programlardan çıkarılması, sertifikalarının Türkiye'deki kullanıcılar dahil dünyadaki tüm tarayıcılarda reddedilmesi anlamına gelir.

8.2. Kişisel Verilerin Korunması ve Siber Güvenlik

6698 sayılı **Kişisel Verilerin Korunması Kanunu**'nun 12. maddesi veri sorumlusunu, kişisel verilerin güvenliğini sağlamak için "uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri" almakla yükümlü kılar. Kanun şifrelemeyi adıyla saymasa da Kurul'un ilk kez Ocak 2018'de yayımlanan ve Nisan 2025'te güncellenen Kişisel Veri Güvenliği Rehberi, şifrelemeyi temel teknik tedbirler arasında göstermektedir (KVKK, 2018a, 2025). Özel nitelikli kişisel veriler için Kurul'un 31.01.2018 tarihli ve 2018/10 sayılı kararı daha açıktır: bu verilerin elektronik ortamda kriptografik yöntemlerle saklanması ve kriptografik anahtarların güvenli ve farklı ortamlarda tutulması gerekir (KVKK, 2018b). Avrupa Birliği Genel Veri Koruma Tüzüğü de şifrelemeyi uygun tedbirler arasında açıkça sayar (m. 32) ve verinin şifreli olduğu ihlallerde ilgili kişilere bildirim yükümlülüğünü kaldırabilir (m. 34/3-a).

Kamu kurumları için bağlayıcı ayrıntı, 2019/12 sayılı Cumhurbaşkanlığı Genelgesi kapsamında Dijital Dönüşüm Ofisi tarafından Temmuz 2020'de yayımlanan **Bilgi ve İletişim Güvenliği Rehberi**'nde yer alır. Rehberin kriptografik algoritmalar ve kullanımı, şifreleme ve anahtar yönetimi ile kriptografik uygulamalar başlıkları, varlık grubuna ve kritiklik derecesine

burakoguz.com

göre tedbirler tanımlar (CBDDO, 2020). 19 Mart 2025 tarihli ve 32846 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 7545 sayılı **Siber Güvenlik Kanunu** ise Siber Güvenlik Başkanlığı'nı kritik altyapılar için standart belirleme ve denetim konusunda yetkilendirmiştir. Kuantum sonrası geçiş takviminin Türkiye'de bu yetki çerçevesinde belirlenmesi beklenen bir adımdır; Tablo 3'te görüldüğü gibi ABD, Birleşik Krallık ve AB takvimlerini ilan etmişken Türkiye için açıklanmış bir takvim bulunmamaktadır.

8.3. Ceza Muhakemesi, Şifreli Deliller ve AYM Kararı

Şifreleme, ceza muhakemesinde de doğrudan sonuç doğurur. 5271 sayılı Ceza Muhakemesi Kanunu'nun 134. maddesinin 7145 sayılı Kanunla değişik ikinci fıkrası, bilgisayar, bilgisayar programları ve kütüklerine "şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması" hâlinde, çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için bu araç ve gereçlere el konulabileceğini ve şifre çözülüp kopyalar alındığında cihazların gecikmeden iade edileceğini düzenler. Kanun koyucunun kullandığı "şifrenin çözümü" ifadesi teknik açıdan dikkatle okunmalıdır. Güçlü tam disk şifrelemesi ve güçlü bir parola söz konusu olduğunda "çözüm" çoğu zaman AES'in kriptanalizi değil, anahtarın başka bir kaynaktan, örneğin çalışan cihazın belleğinden, TPM'den, bulut yedeğinden ya da kurtarma anahtarından elde edilmesi anlamına gelir. Bu yollar kapalıysa, serinin birinci bölümünde açıklanan hesaplamalı güvenlik nedeniyle "işlemin uzun sürmesi" makul bir süre içinde sonuç vermeyebilir.

Anayasa Mahkemesi 12 Şubat 2026 tarihli, E.2023/128, K.2026/36 sayılı kararıyla, maddenin bilgisayarlarda arama, kopyalama ve şifre çözümüne ilişkin birinci fıkrasının ve şifre çözülemediğinde el koymaya ilişkin ikinci fıkrasının ilgili kısımlarını Anayasa'nın 13. ve 20. maddelerine aykırı bularak iptal etmiştir. Mahkeme, soruşturmada elde edilen dijital verilerin saklanma süresi, silinmesi ve işlenmesinin sınırları konusunda kanunda yeterli güvence bulunmadığını tespit etmiştir. Karar 25 Mayıs 2026 tarihli ve 33264 sayılı Resmî Gazete'de yayımlanmış; iptalin doğuracağı boşluğun kamu yararını zedeleyeceği gerekçesiyle yürürlüğü dokuz ay ertelenerek 25 Şubat 2027 olarak belirlenmiştir (Anayasa Mahkemesi, 2026). Bu tarihe kadar yapılacak yasal düzenlemenin, şifreli cihazlardan elde edilen verinin saklanması ve imhası konusunda kriptografik açıdan da somut kurallar içermesi beklenmektedir.

Bilirkişilik uygulaması açısından iki sonuç çıkarılabilir. Birincisi, raporlarda şifrelemenin türü, kullanılan algoritma ve anahtarın elde edilip edilemeyeceği somut olarak belirtilmeli; "şifreli olduğu için incelenemedi" gibi genel ifadelerden kaçınılmalıdır. İkincisi, alınan imajların bütünlüğü MD5 yerine ya da onunla birlikte SHA-256 ile belgelenmeli, özet değerleri serinin birinci bölümündeki Örnek 6'da gösterildiği gibi iki bağımsız araçla çapraz doğrulanmalıdır. Sertifika Şeffaflığı kayıtları (Kısım 2.3) ve dijital imzalar da delilin kaynağını ve zamanını gösteren bağımsız kanıtlar olarak rapora eklenebilir.

Uluslararası düzeyde kriptografik ürünlerin ihracatı, Türkiye'nin de katıldığı Wassenaar Düzenlemesi'nin çift kullanımlı ürünler listesinin 5. kategori 2. kısmında kontrol altına alınmıştır. Kitlesel pazar yazılımları ve açık kaynak kütüphaneler için önemli istisnalar bulunsa da özel kripto ürünleri geliştiren firmaların ihracat öncesinde bu rejimi dikkate alması gerekir.

burakoglun.com

9. Öneriler

Bu derlemenin bulguları, kurumlar ve yazılım geliştiriciler için aşağıdaki somut adımlara dönüştürülebilir:

- **Kriptografik envanter çıkarılmalı.** Hangi sistemin hangi algoritmayı, hangi anahtar uzunluğunu ve hangi kütüphaneyi kullandığı bilinmeden ne SHA-1 temizliği ne de kuantum sonrası geçiş planlanabilir. Envanter, sertifikaları, VPN yapılandırmalarını, veritabanı şifrelemesini ve gömülü cihazları kapsamalıdır. NCSC takvimi bu işin 2028'e kadar bitirilmesini öngörmektedir.
- **Güncel varsayılanlar benimsenmeli.** Yeni sistemlerde veri şifrelemesi için AES-256-GCM veya ChaCha20-Poly1305, özet için SHA-256, SHA-512 veya SHA-3, imza için Ed25519 veya ECDSA P-256, anahtar değişimi için X25519MLKEM768, parola saklama için Argon2id kullanılmalıdır. DES, 3DES, RC4, MD5, SHA-1 ve 1024 bitlik RSA/DH envanterden temizlenmelidir.
- **Kripto çeviklik (crypto-agility) tasarıma katılmalı.** Algoritma adları kodun içine gömülmemeli, yapılandırmayla değiştirilebilir olmalıdır. SHA-1'den kurtulmak on yıldan uzun sürdü; kuantum sonrası geçişte aynı süreye sahip değiliz.
- **Sertifika yenileme otomatikleştirilmeli.** 15 Mart 2027'den itibaren 100 günlük, 2029'dan itibaren 47 günlük sertifika ömrü elle yönetilemez. ACME protokolüne dayalı otomasyon kurulmalı ve alan adları Sertifika Şeffaflığı kayıtları üzerinden izlenmelidir.
- **Uzun ömürlü veriler önceliklendirilmeli.** On yıldan uzun süre gizli kalması gereken veriler (sağlık, nüfus, savunma, ticari sır) için hibrit kuantum sonrası anahtar değişimi 2026-2027 içinde devreye alınmalıdır. Serinin birinci bölümündeki ölçümler bunun işlemci açısından bir engel oluşturmadığını göstermektedir; ağ cihazlarının büyük ClientHello mesajlarını doğru işleyip işlemediği ise önceden test edilmelidir.
- **Kendi kriptografinizi yazmayın.** İncelenmiş kütüphaneler kullanılmalı, nonce üretimi, rastgele sayı kaynağı ve anahtar saklama gibi uygulama ayrıntıları bağımsız kod incelemesinden geçirilmeli, anahtarlar mümkünse HSM veya TPM gibi donanım modüllerinde tutulmalıdır. Kamu şartnamelerindeki FIPS 140-2 atıfları FIPS 140-3 olarak güncellenmelidir.
- **Parolasız kimlik doğrulamaya geçilmeli.** Kurumsal ve kamu hizmetlerinde oltalamaya dayanıklı WebAuthn geçiş anahtarları, SMS ile gönderilen tek kullanımlık kodların yerini almalıdır.
- **Ulusal takvim netleştirilmeli.** Siber Güvenlik Başkanlığı, BTK ve Kamu SM'nin kamu ve kritik altyapılar için kuantum sonrası geçiş takvimini ve e-imza mevzuatındaki algoritma güncellemesini birlikte ilan etmesi, sektörün yatırım planlaması için gereklidir. CMK m. 134'ün yeniden düzenlenmesi sürecinde de şifreli dijital delillerin saklanması ve imhasına ilişkin teknik kuralların kriptografi uzmanlarının katkısıyla belirlenmesi yararlı olacaktır.

burakoksuz.com

10. Sonuç

Serinin birinci bölümü, bugün kullanılan simetrik algoritmaların ve özet fonksiyonlarının sağlam olduğunu, kırılmaların ise çoğunlukla uygulamadan kaynaklandığını göstermişti. Bu ikinci bölüm, aynı tespitin sistem düzeyinde de geçerli olduğunu ortaya koymaktadır. DigiNotar'da bir sertifika otoritesinin sunucuları, TÜRKTRUST'ta bir idari süreç, Heninger ve arkadaşlarının taramasında gömülü cihazların rastgele sayı üreteçleri, Clipper çipinde ise 16 bitlik bir sağlama değeri zincirin en zayıf halkası olmuştur. Hiçbirinde AES ya da RSA'nın matematiği kırılmamıştır.

Değişmesi gereken, açık anahtarlı katmandır ve bu değişim anahtar değişiminde fiilen başlamıştır. Tarayıcılar, OpenSSL 3.5 ve OpenSSH 10 hibrit ML-KEM'i varsayılan hâle getirmiş; serinin birinci bölümündeki ölçümler bu geçişin işlemci açısından bir yük getirmediğini göstermiştir. İmzalarda ise hem boyut hem hız nedeniyle geçiş daha yavaş ilerleyecektir. Sertifika ömürlerinin 2029'da 47 güne inmesiyle zorunlu hâle gelecek otomasyon, imzaların kuantum sonrası algoritmalara taşınmasını da kolaylaştıracaktır. ABD, Birleşik Krallık ve Avrupa Birliği takvimlerinin 2030-2035 aralığında buluşması, bu işin bir on yıl içinde tamamlanması gerektiğini göstermektedir.

Türkiye açısından önümüzdeki dönemin gündemi belirgindir: kuantum sonrası geçiş için ulusal bir takvim ilan edilmesi, e-imza mevzuatının yeni algoritmalara açılması ve Anayasa Mahkemesi'nin iptal kararı sonrasında CMK m. 134'ün, şifreli dijital delillerin teknik gerçekliğini dikkate alan bir biçimde 25 Şubat 2027'ye kadar yeniden düzenlenmesi. Bu üç başlığın ortak paydası, hukuk ile kriptografi arasında daha sıkı bir diyalog kurulmasıdır. Kurumların önündeki asıl iş ise yeni algoritmaları öğrenmekten çok, hangi algoritmanın nerede ve nasıl kullanıldığını bilmek ve bunu değiştirebilecek esnekliği sistemlerine kazandırmaktır.

Kaynakça

Aas, J., Barnes, R., Case, B., Durumeric, Z., Eckersley, P., Flores-López, A., Halderman, J. A., Hoffman-Andrews, J., Kasten, J., Rescorla, E., Schoen, S., & Warren, B. (2019). Let's Encrypt: An automated certificate authority to encrypt the entire web. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 2473-2487). https://doi.org/10.1145/3319535.3363192

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M. A., & Weitzner, D. J. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. Journal of Cybersecurity, 1(1), 69-79. https://doi.org/10.1093/cybsec/tyv009

Anayasa Mahkemesi. (2026). E.2023/128, K.2026/36 sayılı karar (12 Şubat 2026). Resmî Gazete, 25 Mayıs 2026, Sayı: 33264.

Apple. (2016, 16 Şubat). A message to our customers. https://www.apple.com/customer-letter/

Apple. (2025). Advanced Data Protection in the UK [Destek belgesi]. https://support.apple.com/en-us/122234

burakoguz.com

Barker, E. (2020). Recommendation for key management: Part 1 - General (NIST Special Publication 800-57 Part 1 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt1r5

Barker, E., & Kelsey, J. (2015). Recommendation for random number generation using deterministic random bit generators (NIST Special Publication 800-90A Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-90Ar1

Barker, E., Kelsey, J., McKay, K., Roginsky, A., & Sönmez Turan, M. (2025). Recommendation for random bit generator (RBG) constructions (NIST Special Publication 800-90C). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-90C

Blaze, M. (1994). Protocol failure in the escrowed encryption standard. In Proceedings of the 2nd ACM Conference on Computer and Communications Security (pp. 59-67). https://doi.org/10.1145/191177.191193

Boemer, F., Tarbe, K., & Rishi, R. (2024, 30 Temmuz). Announcing Swift Homomorphic Encryption. Swift.org. https://www.swift.org/blog/announcing-swift-homomorphic-encryption/

CA/Browser Forum. (2025, 11 Nisan). Ballot SC081v3: Introduce schedule of reducing validity and data reuse periods. https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/

Castryck, W., & Decru, T. (2023). An efficient key recovery attack on SIDH. In Advances in Cryptology - EUROCRYPT 2023, LNCS 14008 (pp. 423-447). Springer. https://doi.org/10.1007/978-3-031-30589-4_15

CBDDO. (2020). Bilgi ve iletişim güvenliği rehberi. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. https://cbddo.gov.tr/bgrehber

Chromium. (2024). Fortinet connections fail with ERR_TIMED_OUT when post-quantum TLS is enabled (Issue 336007383). https://issues.chromium.org/issues/336007383

Cooper, D. A., Apon, D. C., Dang, Q. H., Davidson, M. S., Dworkin, M. J., & Miller, C. A. (2020). Recommendation for stateful hash-based signature schemes (NIST Special Publication 800-208). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-208

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile (RFC 5280). Internet Engineering Task Force. https://doi.org/10.17487/RFC5280

Council of the European Union. (2025, 26 Kasım). Child sexual abuse: Council reaches position on law protecting children from online abuse [Basın duyurusu]. https://www.consilium.europa.eu/en/press/press-releases/2025/11/26/child-sexual-abuse-council-reaches-position-on-law-protecting-children-from-online-abuse/

Donenfeld, J. A. (2017). WireGuard: Next generation kernel network tunnel. In Network and Distributed System Security Symposium (NDSS 2017). https://doi.org/10.14722/ndss.2017.23160

European Parliament. (2026). Legislative train: Combating child sexual abuse online (2022/0155(COD)). https://www.europarl.europa.eu/legislative-train/spotlight-JD22/file-combating-child-sexual-abuse-online

burakolgun.com

FIDO Alliance. (2026, 7 Mayıs). Five billion passkeys: FIDO Alliance reports mainstream global usage on World Passkey Day 2026. https://fidoalliance.org/fido-alliance-reports-accelerating-global-passkey-adoption-on-world-passkey-day-2026/

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In Proceedings of the 41st Annual ACM Symposium on Theory of Computing (pp. 169-178). https://doi.org/10.1145/1536414.1536440

Gidney, C. (2025). How to factor 2048 bit RSA integers with less than a million noisy qubits. arXiv. https://arxiv.org/abs/2505.15917

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 5, 433. https://doi.org/10.22331/q-2021-04-15-433

Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. SIAM Journal on Computing, 18(1), 186-208. https://doi.org/10.1137/0218012

Google Chrome. (tarihsiz). Certificate Transparency in Chrome. https://googlechrome.github.io/CertificateTransparency/

Groth, J. (2016). On the size of pairing-based non-interactive arguments. In Advances in Cryptology - EUROCRYPT 2016, LNCS 9666 (pp. 305-326). Springer. https://doi.org/10.1007/978-3-662-49896-5_11

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the 28th Annual ACM Symposium on Theory of Computing (pp. 212-219). https://doi.org/10.1145/237814.237866

Heninger, N., Durumeric, Z., Wustrow, E., & Halderman, J. A. (2012). Mining your Ps and Qs: Detection of widespread weak keys in network devices. In 21st USENIX Security Symposium (pp. 205-220). USENIX Association. https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/heninger

Hoogstraaten, H., Prins, R., Niggebrugge, D., Heppener, D., Groenewegen, F., Wettinck, J., Strooy, K., Arends, P., Pols, P., Kouprie, R., Moorrees, S., van Pelt, X., & Hu, Y. Z. (2012). Black Tulip: Report of the investigation into the DigiNotar certificate authority breach (v1.0). Fox-IT BV.

Huelsing, A., Butin, D., Gazdag, S., Rijneveld, J., & Mohaisen, A. (2018). XMSS: eXtended Merkle signature scheme (RFC 8391). Internet Engineering Task Force. https://doi.org/10.17487/RFC8391

ISO/IEC. (2015). ISO/IEC 11889-1:2015 Information technology - Trusted platform module library - Part 1: Architecture. International Organization for Standardization.

Josefsson, S., & Liusvaara, I. (2017). Edwards-curve digital signature algorithm (EdDSA) (RFC 8032). Internet Engineering Task Force. https://doi.org/10.17487/RFC8032

KVKK. (2018a). Kişisel veri güvenliği rehberi (teknik ve idari tedbirler). Kişisel Verileri Koruma Kurumu. https://www.kvkk.gov.tr

KVKK. (2018b). Özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler (Kurul Kararı 2018/10, 31.01.2018). Resmî Gazete, 7 Mart 2018, Sayı: 30353.

KVKK. (2025). Kişisel veri güvenliği rehberi (teknik ve idari tedbirler) (Yayın No: 72, güncellenmiş baskı). Kişisel Verileri Koruma Kurumu. https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf

burakolgun.com

Langley, A. (2013, 3 Ocak). Enhancing digital certificate security. Google Online Security Blog. https://security.googleblog.com/2013/01/enhancing-digital-certificate-security.html

Langley, A., Hamburg, M., & Turner, S. (2016). Elliptic curves for security (RFC 7748). Internet Engineering Task Force. https://doi.org/10.17487/RFC7748

Laurie, B., Langley, A., & Kasper, E. (2013). Certificate Transparency (RFC 6962). Internet Engineering Task Force. https://doi.org/10.17487/RFC6962

Laurie, B., Messeri, E., & Stradling, R. (2021). Certificate Transparency version 2.0 (RFC 9162). Internet Engineering Task Force. https://doi.org/10.17487/RFC9162

Lenstra, A. K., Hughes, J. P., Augier, M., Bos, J. W., Kleinjung, T., & Wachter, C. (2012). Public keys. In Advances in Cryptology - CRYPTO 2012, LNCS 7417 (pp. 626-642). Springer. https://doi.org/10.1007/978-3-642-32009-5_37

Let's Encrypt. (2025, 6 Ağustos). OCSP service has reached end of life. https://letsencrypt.org/2025/08/06/ocsp-service-has-reached-end-of-life

Let's Encrypt. (2026). Let's Encrypt stats [Veri seti, erişim: 28 Eylül 2026]. https://letsencrypt.org/stats/

Marlinspike, M., & Perrin, T. (2016). The Double Ratchet algorithm (Revision 1). Signal. https://signal.org/docs/specifications/doubleratchet/

McGrew, D., Curcio, M., & Fluhrer, S. (2019). Leighton-Micali hash-based signatures (RFC 8554). Internet Engineering Task Force. https://doi.org/10.17487/RFC8554

Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D. (2024). Transition to post-quantum cryptography standards (NIST IR 8547 initial public draft). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8547.ipd

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38-41. https://doi.org/10.1109/MSP.2018.3761723

Mozilla. (2013, 3 Ocak). Revoking trust in two TurkTrust certificates. Mozilla Security Blog. https://blog.mozilla.org/security/2013/01/03/revoking-trust-in-two-turktrust-certficates/

Mozilla. (2024). Enable mlkem768x25519 by default (Bugzilla 1919097). https://bugzilla.mozilla.org/show_bug.cgi?id=1919097

NCSC. (2025, 20 Mart). Timelines for migration to post-quantum cryptography. National Cyber Security Centre. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

NIS Cooperation Group. (2025). A coordinated implementation roadmap for the transition to post-quantum cryptography. European Commission. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

NIST. (2019). Security requirements for cryptographic modules (FIPS PUB 140-3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.140-3

NIST. (2024a). Module-lattice-based key-encapsulation mechanism standard (FIPS PUB 203). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.203

NIST. (2024b). Module-lattice-based digital signature standard (FIPS PUB 204). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.204

NIST. (2024c). Stateless hash-based digital signature standard (FIPS PUB 205). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.205

burakolgun.com

NIST. (2025, 11 Mart). NIST selects HQC as fifth algorithm for post-quantum encryption [Basın duyurusu]. https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

NIST. (tarihsiz). FIPS 140-3 transition effort. Computer Security Resource Center. https://csrc.nist.gov/projects/fips-140-3-transition-effort

OpenSSH. (2025). OpenSSH 10.0 release notes. https://www.openssh.com/releasenotes.html

Rescorla, E. (2018). The Transport Layer Security (TLS) protocol version 1.3 (RFC 8446). Internet Engineering Task Force. https://doi.org/10.17487/RFC8446

Sectigo. (tarihsiz). TLS/SSL certificate lifespan history (2, 3, and 5-year validity). https://www.sectigo.com/knowledge-base/detail/TLS-SSL-Certificate-Lifespan-History-2-3-and-5-year-validity/kA01N000000zFKp

Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613. https://doi.org/10.1145/359168.359176

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (pp. 124-134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

Sönmez Turan, M., Barker, E., Kelsey, J., McKay, K. A., Baish, M. L., & Boyle, M. (2018). Recommendation for the entropy sources used for random bit generation (NIST Special Publication 800-90B). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-90B

Swihart, J. (2019, 5 Şubat). Zcash counterfeiting vulnerability successfully remediated. Electric Coin Company. https://electriccoin.co/blog/zcash-counterfeiting-vulnerability-successfully-remediated/

Telekomünikasyon Kurumu. (2005). Elektronik imza ile ilgili süreçlere ve teknik kriterlere ilişkin tebliğ. Resmî Gazete, 6 Ocak 2005, Sayı: 25692.

tldr.fail. (tarihsiz). tldr.fail: Your server is not reading the whole ClientHello. https://tldr.fail/

Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd. In 2020 IEEE Symposium on Security and Privacy (pp. 517-533). https://doi.org/10.1109/SP40000.2020.00031

W3C. (2021, 8 Nisan). Web Authentication: An API for accessing public key credentials - Level 2 (W3C Recommendation). https://www.w3.org/TR/webauthn-2/

W3C. (2026, 25 Ağustos). Web Authentication: An API for accessing public key credentials - Level 3 (W3C Recommendation). https://www.w3.org/TR/webauthn-3/

Westerbaan, B. (2025, 28 Ekim). State of the post-quantum Internet in 2025. Cloudflare Blog. https://blog.cloudflare.com/pq-2025/

Westerbaan, B. (2026, 7 Nisan). Cloudflare targets 2029 for full post-quantum security. Cloudflare Blog. https://blog.cloudflare.com/post-quantum-roadmap/

Yao, A. C. (1982). Protocols for secure computations. In 23rd Annual Symposium on Foundations of Computer Science (pp. 160-164). IEEE. https://doi.org/10.1109/SFCS.1982.38

burakolgun.com