T.C.
IŞIK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
SİBER GÜVENLİK PROGRAMI

Erdem ULUTAŞ

PAROLA KARMA ALGORİTMALARININ DERİNLEMESİNE KARŞILAŞTIRMASI: KRİPTOGRAFİK GÜVENLİK, PERFORMANS ETKİNLİĞİ, REGÜLASYON UYUMLULUĞU VE ANAHTAR TÜRETİM STRATEJİLERİNDE GELECEK EĞİLİMLER

DANIŞMAN
Dr. Öğr. Üyesi Barış ÇELİKTAŞ

İSTANBUL, Haziran 2025

T.C.
IŞIK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
SİBER GÜVENLİK PROGRAMI

Erdem ULUTAŞ

(23SİBE5003)

PAROLA KARMA ALGORİTMALARININ DERİNLEMESİNE KARŞILAŞTIRMASI: KRİPTOGRAFİK GÜVENLİK, PERFORMANS ETKİNLİĞİ, REGÜLASYON UYUMLULUĞU VE ANAHTAR TÜRETİM STRATEJİLERİNDE GELECEK EĞİLİMLER

DANIŞMAN

Dr. Öğr. Üyesi Barış ÇELİKTAŞ

İSTANBUL, Haziran 2025

T.C.
IŞIK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
SİBER GÜVENLİK PROGRAMI

Erdem ULUTAŞ
(23SİBE5003)

PAROLA KARMA ALGORİTMALARININ DERİNLEMESİNE KARŞILAŞTIRMASI: KRİPTOGRAFİK GÜVENLİK, PERFORMANS ETKİNLİĞİ, REGÜLASYON UYUMLUĞU VE ANAHTAR TÜRETİM STRATEJİLERİNDE GELECEK EĞİLİMLER

Tezin Savunulduğu Tarih: 30/06/2025

Tez Danışmanı: Dr. Öğr. Üyesi Barış ÇELİKTAŞ / Işık Üniversitesi

Diğer Jüri Üyeleri: Dr. Öğr. Üyesi Emine Ekin / Işık Üniversitesi

Prof. Dr. Enver Özdemir / İstanbul Teknik Üniversitesi

İSTANBUL, Haziran 2025

ÖZET

PAROLA KARMA ALGORİTMALARININ DERİNLEMESİNE KARŞILAŞTIRMASI: KRİPTOGRAFİK GÜVENLİK, PERFORMANS ETKİNLİĞİ, REGÜLASYON UYUMLUĞU VE ANAHTAR TÜRETİM STRATEJİLERİNDE GELECEK EĞİLİMLER

Parola karma ve anahtar türetme fonksiyonlarının uygulanması, kullanıcı kimlik bilgilerinin kaba kuvvet saldırılarına ve yetkisiz erişime karşı korunmasını amaçlayan kimlik doğrulama ve kriptografik güvenlik şemalarının temelini oluşturmaktadır. PBKDF2, bcrypt ve scrypt gibi parola karma algoritmaları günümüzde oldukça popüler olmasına rağmen modern donanımdaki gelişmeler, paralel işlem yetenekleri ve gelişmiş kriptoanalitik saldırılar karşısında yetersiz kalmaktadır. Bu eksiklikleri gidermek amacıyla, 2013 yılında parola karma yarışması başlatılmış ve parola karma için 22 aday fonksiyonel değerlendirmeye alınmıştır. Yapılan kapsamlı incelemeler sonucunda, güvenlik, hız, bellek dostu olma, esneklik ve verimlilik kriterlerine dayanarak 9 finalist belirlenmiştir. Bu çalışma, parola karma yarışması finalistleri olan Argon, battcrypt, Catena, Lyra2, MAKWA, Parallel, POMELO, Pufferfish ve yescrypt üzerine yapılan derleme ve performans değerlendirme çalışmalarını ele almaktadır. Finalistler mimari açıdan değerlendirilmiş, güvenlik özellikleri, bellek kullanım dayanıklılığı, performans açısından avantaj ve dezavantajları ayrıca pratik kullanımları incelenmiştir. Bu yeni fonksiyonların geleneksel parola karma algoritmaları ile kıyaslanarak eksiklikleri ve avantajları ortaya konmuştur. Parola karma algoritmalarının kuantum sonrası dayanıklılığı ele alınarak, bu fonksiyonların kuantum saldırılarına karşı dayanıklılığı ve ek bir güvenlik önlemi olarak kullanılan "peppering" tekniğinin rolü araştırılmıştır. Ayrıca parola karma yarışması

finalistlerinin NIST SP 800-63B, OWASP ASVS, PCI DSS, GDPR, KVKK ve ISO/IEC 27001 gibi küresel standartlar ve regülasyonlarla olan uyumluluklarını kapsamlı bir şekilde haritalandırılarak, regülasyonlara uyumlu olması gereken organizasyonlarda güvenli dağıtım için pratik uygunlukları değerlendirilmiştir. Son olarak, web kimlik doğrulaması, anahtar türetme fonksiyonları ve gömülü platformlar için bu fonksiyonların kullanımına yönelik öneriler sunulmuştur. Bu çalışmanın amacı, en güncel parola karma ve anahtar türetme fonksiyonları hakkında bilgi sahibi olması gereken araştırmacılar, geliştiriciler ve güvenlik mühendisleri için bir referans kaynağı olmaktır.

Anahtar Kelimeler: Parola Karma, Anahtar Türetme, Güvenlik, Kuantum Dayanıklılığı, Uyumluluk

ABSTRACT

COMPARATIVE ANALYSIS OF PASSWORD HASHING COMPETITION FINALISTS: SECURITY, EFFICIENCY, COMPLIANCE, AND FUTURE TRENDS IN KEY DERIVATION

The application of password hashes and key derivation functions (KDFs) is core to authentication and cryptographic security schemes crafted to defend user credentials from brute-force attacks and unauthorized access. Password hashing algorithms, for example PBKDF2, bcrypt, or scrypt, are very popular today, but are lacking in the face of modern hardware acceleration, parallel processing, and advanced cryptanalytic attacks. To contest these shortcomings, the Password Hashing Competition (PHC) was started in 2013 and had 22 candidates for functions for hashing passwords. After thorough evaluation, 9 finalists were selected based on how secure, fast, memory-friendly, flexible, and efficient these functions were. This study discusses the survey and benchmark studies of the PHC finalists: Argon, battcrypt, Catena, Lyra2, MAKWA, Parallel, POMELO, Pufferfish, and yescrypt. We have evaluated these functions from an architectural standpoint and studied their security features, memory hardness, performance trade-off, and practical usage. These functions also need to be compared with traditional password hashing functions, and this was done to evaluate the new functions' flaws and advantages. We also investigate the post-quantum assumption for password hashing – the effectiveness of these functions against quantum assaults, their position in a new cryptography set, and the role of peppering as an additional security measure. In addition, we perform a comprehensive compliance mapping of the PHC finalists against major global standards and regulations such as NIST SP 800-63B, OWASP ASVS, PCI DSS, GDPR, KVKK, and ISO/IEC 27001, highlighting their practical suitability for

secure deployment in regulated environments. Finally, we provide usage recommendations for these functions for web authentication, KDFs, and embedded platforms. The purpose of this paper is to serve as a reference for researchers, developers, and security engineers who need to have a solid grasp of state-of-the-art password hashing and key derivation techniques.
Keywords: Password Hashing, Key Derivation, Security, Quantum Resistance, Compliance

TEŞEKKÜR

Yüksek lisans eğitimim süresince bilgi ve tecrübeleriyle bana her zaman yol gösteren, akademik gelişimime katkıda bulunan, değerli görüşleriyle tezimin şekillenmesinde büyük rol oynayan danışmanım Dr. Öğr. Üyesi Barış ÇELİKTAŞ'a en içten teşekkürlerimi sunarım. Sabırlı yaklaşımı, yapıcı eleştirileri ve desteğiyle bu süreci daha verimli ve anlamlı hale getirmiştir. Ayrıca, her daim yanımda olan, desteğini ve sevgisini hiçbir zaman esirgemeyen kıymetli aileme de sonsuz teşekkür ederim. Varlıkları, motivasyonumu her zaman yüksek tutmamı sağladı ve bu süreci başarıyla tamamlamamda en büyük paya sahip oldular.

Erdem ULUTAŞ

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

KISALTMALAR LİSTESİ

ASIC: Application-Specific Integrated Circuit

ASVS: Application Security Verification Standard

BGYS: Bilgi Güvenliği Yönetim Sistemi

CCPA: California Consumer Privacy Act

CSPRNG: Cryptographically Secure Pseudorandom Number Generator

ECC: Elliptic Curve Cryptography

FIPS-140: Federal Information Processing Standard 140

FPGA: Field-Programmable Gate Array

GB: Gigabyte

GDPR: General Data Protection Regulation

GPU: Graphics Processing Unit

HMAC: Hash-Based Message Authentication Code

HSM: Hardware Security Module

HUIU: Hash Password Upgrade Independent From the User

IOT: Internet of Things

ISMS: Information Security Management System

ISO/IEC: International Organization for Standardization / International Electrotechnical Commission

KB: Kilobyte

KDF: Key Derivation Function

KVKK: Kişisel Verileri Koruma Kanunu

LGPD: Lei Geral de Proteção de Dados

MAX: Maximum

MB: Megabyte

MFA: Multi-Factor Authentication

MH: Memory-Hard

MHF: Memory-Hard Function

MIN: Minimum

MS: Millisecond

NIST: National Institute of Standards and Technology

OWASP: Open Worldwide Application Security Project

PCI DSS: Payment Card Industry Data Security Standard

PHC: Password Hashing Competition

PIPL: Personal Information Protection Law

PIPEDA: Personal Information Protection and Electronic Documents Act

PR: Pseudorandom

PRNG: Pseudorandom Number Generator

RAM: Random Access Memory

ROM: Read-Only Memory

RSA: Rivest–Shamir–Adleman

SCR: Secure Channel Resistence

TOM: Technical and Organizational Measures

BÖLÜM 1

1. GİRİŞ

Parola karması, modern güvenlik sistemlerinin temel bileşenlerinden birini oluşturmakta olup; kimlik doğrulama, oturum yönetimi ve gizli verilerin saklanması gibi kritik işlevlerde merkezi bir rol oynamaktadır. Kimlik doğrulama sistemlerinde, parolaların karma halinde saklanması, veri tabanının ele geçirilmesi durumunda dahi ek bir koruma katmanı sağlamaktadır (Yao ve Yin, 2005).

Parola karma yöntemlerinde sağlanan ilerlemelere rağmen, kaba kuvvet (brute-force), sözlük tabanlı (dictionary) ve gökkuşağı tablosu (rainbow table) saldırıları gibi çeşitli güvenlik açıkları halen varlığını sürdürmektedir (Luo vd., 2021). Yaygın olarak kullanılan MD5, SHA-1 ve SHA-256 gibi kriptografik karma fonksiyonları, veri bütünlüğünü doğrulamada hızlı çalışacak şekilde tasarlanmıştır. Ancak bu özellik, söz konusu fonksiyonları, yüksek hızlarından faydalanarak geniş ölçekli parola tahmin saldırıları gerçekleştirebilen saldırganlar için cazip hedefler haline getirmektedir (Andrade vd., 2016). Ayrıca, bu fonksiyonların entegre tuzlama (salting) mekanizmaları ve bellek zorlukları içermemesi, önceden hesaplanmış saldırılara karşı savunmasız kalmalarına neden olmaktadır (Álvarez ve Zamora, 2017). Parola saklama süreçlerine "biber" (pepper) mekanizmasının dahil edilmesi, çevrimdışı saldırı risklerini azaltarak güvenliği artırmakta; çünkü veri tabanı ele geçirilse dahi, biber bilgisi saldırganlar tarafından bilinmemektedir (Blocki ve Sridhar, 2016). Zamanlama saldırıları gibi yan kanal saldırıları da, sistem davranışları üzerinden kriptografik işlemlere dair hassas bilgilerin sızmasına yol açarak ek riskler oluşturmaktadır (Alwen vd., 2018).

Anahtar türetme fonksiyonları (KDF'ler), zayıf kullanıcı parolalarını güçlü kriptografik anahtarlara dönüştürerek şifreleme ve güvenli iletişim protokollerinin etkinliğini artırmaktadır (Grassi vd., 2023). Mevcut KDF'ler—

PBKDF2, bcrypt ve scrypt gibi—donanım düzeyindeki optimizasyonlara karşı savunmasız olup, parola kırma işlemlerinin hesaplama maliyetini düşürebilmektedir. Örneğin, PBKDF2 bellek zorlayıcı (memory-hard) olmaması nedeniyle donanım hızlandırmalı kaba kuvvet saldırılarına karşı açık durumdadır (Alwen vd., 2018). bcrypt farklı hesaplama yüklerini desteklese de, alan programlanabilir kapı dizileri (FPGA) aracılığıyla optimize edilebilmektedir (Luo vd., 2021). Paralel saldırılara karşı dayanıklılık sağlayan scrypt dahi, belirli bellek temelli saldırılara karşı hassasiyet göstermektedir (Choe vd., 2019).

Bu sınırlamaların üstesinden gelmek amacıyla, 2013 yılında daha dayanıklı parola karma şemalarının geliştirilmesini teşvik etmek üzere küresel ölçekte bir girişim olarak PHC (Password Hashing Competition) başlatılmıştır. Toplam 22 aday, güvenlik, bellek zorluk seviyesi, performans ve uygulama esnekliği gibi kriterler doğrultusunda değerlendirilmiştir (Aumasson, 2013). Değerlendirme süreci sonucunda, Argon, battcrypt, Catena, Lyra2, MAKWA, Parallel, POMELO, Pufferfish ve yescrypt olmak üzere dokuz finalist belirlenmiştir. Bu finalistler, kaba kuvvet saldırılarına karşı önemli düzeyde direnç ve pratik uygulama olanakları sunmaktadır (Hatzivasilis vd., 2015).

Bu çalışma, PHC finalistlerini mimari tasarımları, güvenlik özellikleri ve gerçek dünya senaryolarındaki uygulanabilirlikleri açısından kapsamlı biçimde inceleyen bir değerlendirme ve kıyaslama çalışması sunmaktadır. Ayrıca, bu fonksiyonlar yaygın olarak bilinen parola karma algoritmalarıyla karşılaştırılmakta; güçlü ve zayıf yönleri detaylandırılmaktadır. Kuantum sonrası güvenlik yönleri kısaca ele alınmakta ve ilerleyen bölümlerde ayrıntılı şekilde tartışılmaktadır. Son olarak, bu çalışma; web kimlik doğrulaması, kriptografik anahtar türetimi ve gömülü sistem güvenliği gibi çeşitli uygulama alanları için somut öneriler sunmaktadır.

Kuantum bilişimdeki gelişmelerin kriptografik güvenliği tehdit etme potansiyeli göz önüne alındığında, bu çalışma aynı zamanda PHC finalistlerinin kuantum tehditlerine karşı dayanıklılıklarını da incelemektedir.

Bu çalışmanın temel katkıları şu şekildedir:

- Dokuz PHC finalisti parola karma fonksiyonunun güvenlik, performans, uyumluluk ve gerçek dünya uygulanabilirliği açısından karşılaştırmalı değerlendirmesi.
- GPU paralelleştirme, yan kanal saldırıları ve donanım optimizasyonları gibi gelişmiş saldırı vektörlerine karşı bu fonksiyonların dayanıklılığına yönelik analiz.
- PHC finalistlerinin NIST SP 800-63B, OWASP ASVS, PCI DSS, GDPR, KVKK ve ISO/IEC 27001 gibi küresel standart ve düzenlemelerle uyumluluğuna dair kapsamlı haritalama.
- Parola karması üzerinde kuantum bilişimin potansiyel etkilerine dair tartışma.
- Geliştiricilere, araştırmacılara ve kurumlara özel güvenlik ve performans gereksinimlerine göre en uygun parola karma fonksiyonunun seçimi konusunda pratik rehberlik.

Bu makale şu şekilde yapılandırılmıştır: Kısım 2, mevcut KDF'lere dair ilgili çalışmaları incelemekte ve bu fonksiyonların güçlü ve zayıf yönlerini ortaya koymaktadır. Kısım 3, parola karması, KDF'ler, tuzlama, biberleme ve bellek zorlayıcı fonksiyonlar (MHF'ler) gibi temel kavramları açıklayan arka plan bilgisini sunmaktadır. Kısım 4, güvenli parola saklama uygulamalarını etkileyen ilgili kriptografik standartlar ve düzenleyici çerçeveleri ortaya koymaktadır. Kısım 5, bu çalışmanın temel bulgularını içermekte olup; PHC finalistlerinin performans karşılaştırmalarını, güvenlik analizlerini ve uyumluluk değerlendirmelerini kapsamaktadır. Son olarak temel sonuçlar özetlenmekte ve ileri çalışmalar için öneriler sunulmaktadır.

BÖLÜM 2

2. LİTERATÜR

Bu bölüm, mevcut KDF araştırmalarının kapsamlı bir değerlendirmesini sunmakta olup, PHC finalistlerinin değerlendirilmesine temel oluşturmak amacıyla önceki çalışmalardan elde edilen bulguları bütünleştirmektedir.

2.1 KDF ARAŞTIRMALARINA GENEL BAKIŞ

Anahtar türetme fonksiyonları (KDF) üzerine yapılan araştırmalar, parola doğrulama, blokzincir güvenliği (Wang vd., 2018) ve mobil şifreleme (Lu vd., 2016) gibi çeşitli alanlardaki güvenlik sorunlarını ele almak üzere önemli ölçüde evrilmiştir. Mevcut literatürün durumunu daha iyi yansıtmak adına, Tablo 2.1 KDF'lerin farklı uygulama alanlarındaki temel çalışmalarını, bulgularını ve sınırlılıklarını özetlemektedir. Bu çalışmalar, kullanıcı odaklı anahtar yönetimi, kriptografik güvenlik, yan kanal saldırılarına karşı direnç ve blokzincir tabanlı güvenlik uygulamaları gibi çeşitli boyutları ele almaktadır.

KDF araştırmalarında öne çıkan ortak bir tema, özellikle gömülü sistemler veya mobil cihazlar gibi kısıtlı ortamlarda güvenlik ile performans arasındaki dengeyi kurma gerekliliğidir. Örneğin, bellek zorlayıcı KDF'ler üzerine yapılan çalışmalar, kaba kuvvet ve veri yakınındaki işlem saldırılarını (near-data processing attacks) azaltmak için artan hesaplama maliyetinin gerekliliğini vurgulamaktadır (Choe vd., 2019). Ancak bu yöntemler, yüksek kaynak tüketimi gibi uygulama zorlukları doğurarak kısıtlı ortamlarda kullanımı sınırlamaktadır. Ayrıca, sahte rastgele sayı üreteçlerine (PRNG) dayalı KDF'ler de araştırılmış olmakla birlikte, uygulama odaklı çalışmaların yetersizliği nedeniyle bu yaklaşımların verimliliği ve gerçek dünya uygunluğu belirsizliğini korumaktadır (McGinthy ve Michaels, 2019).

Ek olarak, blokzincir tabanlı karma şemaları ve parola tabanlı kriptografik işlevlere dair güvenlik değerlendirmeleri, gerçek dünya dağıtım senaryolarında bazı boşluklara işaret etmektedir. Bazı çalışmalar, kullanıcı gizliliğini artırmak amacıyla anonimlik özellikleri ve PBKDF2 gibi kriptografik yapıtaşlarını içeren doğrulama şemalarında iyileştirmeler önermiştir (Saad vd., 2016). Ancak bu çözümler, gelişmiş tehditlere karşı dayanıklılıklarını değerlendirmek üzere daha fazla ampirik doğrulama ve büyük ölçekli uygulama çalışmaları gerektirmektedir. Genel olarak, KDF araştırmaları kayda değer ilerleme kaydetmiş olsa da, gelecekteki çalışmaların performans optimizasyonunu güvenlikten ödün vermeden sağlamaya odaklanması gerekmektedir.

Tablo 2.1 KDF Üzerine Önceki Çalışmaların Özeti

Referans	**Odak Alanı**	**Temel Bulgular**	**Sınırlılıklar**
Tran vd. (2024)	Kullanıcı Merkezli Anahtar Yönetimi	Anahtar türetimi için KDF kullanan bir bulut şifreleme şeması önerdi.	Büyük ölçekli bulut ortamlarında sınırlı değerlendirme.
Clark ve Seamons (2022)	Parola ve Kriptografik Güvenlik	Parola tabanlı kimlik doğrulama şemalarının teorik sınırlarını araştırdı.	Pratik uygulamalardan ziyade teorik yönlere odaklanıldı.
Kodwani vd. (2021)	Parola Tabanlı Kriptografi	Parola tabanlı kimlik doğrulamada KDF'lerin güvenlik yönleri değerlendirdi.	Farklı KDF uygulamaları için performans kıyaslamaları dahil edilmedi.
Lata ve Bansal (2021)	Yan Kanal Saldırı Direnci	Zamanlama tabanlı yan kanal saldırılarına dayanıklı, güvenli KDF'ler önerdi.	Gerçek dünyadaki dağıtım zorlukları hakkında sınırlı tartışma.

Tablo 2.1 (Devamı) KDF Üzerine Önceki Çalışmaların Özeti

Referans	Odak Alanı	Temel Bulgular	Sınırlılıklar
Luo vd. (2021)	Blok zinciri Tabanlı Siber Güvenlik	Blok zinciri tabanlı güvenlik uygulamaları için hafızaya dayalı bir KDF tanıttı.	Kaynak kısıtlı cihazlar için yüksek hesaplama maliyeti.
Choe vd. (2019)	Bellek-Hard KDF'ler	Scrypt algoritmasının veri-yanında işlem saldırılarına karşı zayıflıkları analiz edilmiştir.	Belirlenen açıklar için karşı önlemler önerilmemiştir.
McGinthy & Michaels (2019)	PRNG Tabanlı KDF'ler	Sahte rasgele sayı üreteçleri (PRNG) kullanılarak anahtar türetme süreçlerinin iyileştirilmesi incelenmiştir.	Teorik güvenliğe odaklanılmış, uygulama verimliliği ele alınmamıştır.
Alwen vd. (2018)	Bellek-Zorlayıcı KDF'ler	Parola karma şemalarının bellek-hardlık özellikleri incelenmiştir.	Farklı donanım mimarilerinde deneysel test yapılmamıştır.
Wang vd. (2018)	Blokzincir Karmalama Güvenliği	Blokzincir bağlamında kullanılan karmalama fonksiyonlarının güvenlik kriterleri incelenmiştir.	KDF'ler blokzincir dışı ortamlarda değerlendirilmemiştir.
Álvarez ve Zamora (2016)	Spritz Tabanlı KDF'ler	Spritz şifresi kullanılarak parola tabanlı KDF tasarımı araştırılmıştır.	Modern donanımlar üzerinde performans değerlendirmesi sınırlıdır.

Tablo 2.1 (Devamı) KDF Üzerine Önceki Çalışmaların Özeti

Referans	Odak Alanı	Temel Bulgular	Sınırlılıklar
Lu vd. (2016)	Mobil Şifreleme Güvenliği	KDF'ler kullanılarak mobil cihazlar için verimli depolama şifrelemesi incelenmiştir.	Farklı mobil platformlar arasında KDF performans karşılaştırması yapılmamıştır.
Saad vd. (2016)	Güvenli Kimlik Doğrulama	Parola tabanlı KDF kullanılan anonim kimlik doğrulama şeması önerilmiştir.	Geniş çaplı bir uygulama sonucu sunulmamıştır.
Forler vd. (2015)	Parola Karma Yarışması	PHC finalistleri, özellikle Argon2, kapsamlı şekilde değerlendirilmiştir.	Gerçek dünyadaki benimseme süreci yerine yarışma sonuçlarına odaklanılmıştır.
Hatzivasilis vd. (2015)	Parola Karma Güvenliği	Parola karmada kullanılan KDF'ler üzerine anket ve kıyaslama çalışması yapılmıştır.	Kuantum sonrası kriptografik değerlendirmeler dahil edilmedi.
Aumasson (2013)	Parola Karmalamanın Geleceği	Parola karmalama ve KDF'lerdeki gelişmeler tartışılmıştır.	Uygulamaya yönelik detaylar yerine teorik analiz ağırlıklıdır.
Yao ve Yin (2005)	Anahtar Türetme Güvenliği	Parola tabanlı KDF'lerin temel güvenlik analizleri yapılmıştır.	Modern donanım hızlandırma saldırılarını öngörememiştir.

2.2 MEVCUT KDF'LERDEKİ SINIRLAMALAR VE ZORLUKLAR

PHC finalistleri, mevcut en sağlam ve güvenli parola karma ve KDF şemalarından bir seçkiyi temsil etmektedir. Bununla birlikte, güvenlik açısından kaydedilen ilerlemelere rağmen, her bir finalist performans, uygulanabilirlik ve genel etkinlik açısından bazı yapısal sınırlılıklar ve zorluklar barındırmaktadır. Bu sınırlamaların başlıca kaynakları arasında bellek kullanımı, hesaplama karmaşıklığı, güvenlik doğrulaması ve farklı ortamlara uyarlanabilirlik yer almaktadır. Tablo 2.2, mevcut PHC finalisti KDF'lerdeki sınırlılıkları ve zorlukları özetlemektedir.

PHC finalistlerinin karşılaştığı temel zorluklardan biri, güvenlik ve verimlilik arasında denge kurmaktır. Argon, Lyra2 ve POMELO gibi bellek zorlayıcı şemalar, gigabayt düzeyinde bellek kullanarak GPU ve ASIC saldırılarına karşı yüksek direnç sunmakla birlikte, kaynak kısıtlı ortamlarda uygulanabilirliği sınırlıdır (Luo vd., 2021). Buna karşın, MAKWA, Parallel ve yescrypt gibi şemalar minimum bellek gerektirirken hesaplama zorluğuna dayanır; bu durum ise belirli donanımlar tarafından istismar edilebilir (Luo vd., 2021). Ayrıca, bazı şemalar (örneğin POMELO) KDF olarak tasarlanmamış olup, anahtar türetme uygulamaları için aynı düzeyde güvenlik sunmamaktadır (Hatzivasilis vd., 2015).

Diğer bir sınırlılık, bazı finalistler için mevcut olan resmi güvenlik doğrulamasının yetersizliğidir. Catena ve Lyra2 gibi fonksiyonlar kapsamlı güvenlik analizlerinden geçirilmişken, battcrypt, Parallel ve yescrypt gibi diğerleri için bu türden resmi güvenlik kanıtları bulunmamaktadır. Pufferfish gibi başka bir finalist, güvenlik özellikleri açısından tam olarak doğrulanmamış olup, saldırgan senaryolarda güvenilirliği konusunda belirsizlikler yaratmaktadır. Ayrıca, POMELO'nun çıktılarında düşük rastgelelik üretmesi, onu güçlü bir KDF olarak uygun olmaktan çıkarmaktadır (Hatzivasilis vd., 2015).

Genel olarak, PHC finalistleri parola karma ve KDF alanında önemli ilerlemeleri temsil etse de, her biri bellek kullanımı, hesaplama yükü ve güvenlik

garantisi açısından farklı ödünleşmeler barındırmaktadır. Bir KDF'nin ideal seçimi, hedef sistemin bağlamsal kısıtları ve hedefleriyle — kaynak kullanımını minimize etmek, yan kanal saldırılarına karşı direnç sağlamak veya kuantum sonrası güvenlik — uyumlu olmalıdır. Bu alandaki gelecekteki gelişmelerin, farklı dağıtım senaryolarında verimlilik ve uyarlanabilirliği koruyarak güvenliği optimize etmeye odaklanması gerekmektedir.

Tablo 2.2 Mevcut KDF'lerdeki (PHC Finalistleri) Sınırlamalar ve Zorluklar

KDF	**Sınırlamalar**	**Zorluklar**
Argon	Güvenlik için yapılandırıldığında yüksek bellek tüketimi	Güvenlik ve performansı dengelemek için parametrelerin dikkatli bir şekilde ayarlanması gerekir
battcrypt	Scrypt'in basitleştirilmiş versiyonu, kullanıcıdan bağımsız tam karma yükseltmesinden (HUIU) yoksundur	Öncelikle sunucu tarafı uygulamaları için tasarlanmıştır, çok yönlülüğü sınırlar
Catena	Scrypt'e kıyasla orta düzeyde bellek tüketimi	Verimlilik darboğazlarından kaçınmak için dikkatli parametre seçimine ihtiyaç vardır
Lyra2	Büyük bellek izi	Kaynak kısıtlı ortamlarda potansiyel verimlilik endişeleri
MAKWA	Büyük sayı aritmetiği nedeniyle hesaplama açısından maliyetli	Karmaşık tasarım, güvenlik için çevrimdışı karma yükseltmesi gerektirir
Parallel	Hesaplama zorluğu var ama bellek zorluğu yok.	Diğer bazı adaylar kadar güvenlik açısından kapsamlı bir şekilde analiz edilmemiştir

Tablo 2.2 (Devamı) Mevcut KDF'lerdeki (PHC Finalistleri) Sınırlamalar ve Zorluklar

KDF	Sınırlamalar	Zorluklar
POMELO	Daha düşük rastgelelik nedeniyle güvenli bir KDF olarak işlev görmez	Güçlü anahtar türetme gerektiren uygulamalar için uygun olmayabilir
Pufferfish	Güvenlik özellikleri tam olarak doğrulanmadı	Diğer bellek-zor KDF'lere kıyasla biraz daha az verimli
yescrypt	Scrypt'e dayalı ancak güvenlik kanıtları eksik	Bellek zorluğu ve hesaplama performansının dengelenmesi

BÖLÜM 3

3. ÖN BİLGİLER

Bu bölüm, parola güvenlik mekanizmalarına ilişkin temel kavramları tanıtmaktadır. Bu kapsamda; karma, anahtar türetme fonksiyonları, tuzlama (salting), biberleme (peppering), bellek zorlayıcı fonksiyonlar gibi yapılar ele alınmakta ve bunların kaba kuvvet saldırılarına karşı sağladığı direnç üzerindeki etkileri tartışılmaktadır. Bu bileşenler, gelişen hesaplama tehditlerine karşı kimlik doğrulama sistemlerinin dayanıklılığını bütüncül biçimde artırmaktadır.

3.1 PAROLA KARMASINA GENEL BAKIŞ

Parola karma, kullanıcı kimlik bilgilerinin korunmasını sağlamak amacıyla düz metin parolaların sabit uzunlukta bir karma değerine dönüştürülmesi sürecidir. Bu işlem, orijinal girdinin geri elde edilmesini hesaplama açısından olanaksız hale getirir (Aumasson, 2013). Karma işlemi, şifrelemeden farklı olarak tek yönlü bir dönüşümdür; yani şifreleme anahtarına sahip bir saldırgan veriyi geri çözebilirken, karma işlemi geri dönüşü mümkün olmayan bir işlem olduğundan, parola saklama ve kimlik doğrulamada tercih edilen yöntemdir (Lu vd., 2016).

Kimlik doğrulama sistemlerinde, saklanan parola karma değerleri kullanıcı tarafından girilen yeni parolanın karma değeri ile karşılaştırılır; orijinal parolanın geri çağrılmasına gerek yoktur. Buna karşın, şifreleme, geri alınabilir verilerin (örneğin kullanıcı bilgilerinin) korunması için daha uygundur (OWASP Password Storage Cheat Sheet, 2025).

3.2 ANAHTAR TÜRETME FONKSİYONLARI

Anahtar Türetme Fonksiyonları (KDF'ler), kullanıcı parolası gibi basit girdilerden güvenli kriptografik anahtarlar üretmek için kullanılır. Yaygın olarak kullanılan KDF'ler arasında PBKDF2 (RFC 6070, 2011) ve bcrypt (Provos ve Mazieres, 1999) bulunmaktadır. Bu fonksiyonlar çok sayıda yineleme (iteration) içerir; ancak bellek zorluğuna sahip değildirler. Argon2 (RFC 9106, 2021) ve Lyra2 (Simplicio vd., 2014) gibi daha modern KDF'ler, güvenliği artırmak amacıyla bellek zorluğunu içeren tasarımlar sunar.

KDF'lerdeki iş faktörü (work factor), parolaya uygulanan yineleme sayısını belirler. Bu değerin artırılması, sözlük ve kaba kuvvet saldırılarını hesaplama açısından daha maliyetli hale getirerek güvenliği güçlendirir (Clark ve Seamons, 2022). Ancak iş faktörünün aşırı yükseltilmesi, sistem performansını düşürebilir ve kimlik doğrulama taleplerinin sunucu kaynaklarını tüketmesi sonucunda hizmet reddi (DoS) riskine yol açabilir (Hatzivasilis vd., 2015).

Güncel tehditleri ele alabilmek amacıyla, Argon2 ve yescrypt gibi modern KDF'ler, ayarlanabilir iş faktörleri sunmaktadır. Bu sayede sistemler zamanla hesaplama maliyetlerini artırabilir. Kimlik doğrulama sırasında parolaların yeniden işlenmesi (rehashing) yoluyla uyumluluk sağlanırken güvenlik de korunur (Clark ve Seamons, 2022). Bu bağlamda, iş faktörlerinin periyodik olarak yeniden değerlendirilmesi, artan hesaplama gücüne karşı önlem olarak önerilmektedir (OWASP Password Storage Cheat Sheet, 2025).

Bu süreci görselleştirmek amacıyla, Şekil 2.1 genel bir KDF algoritmasının sadeleştirilmiş sözde kodunu göstermektedir. Bu modelde, tuzlama, yineleme döngüleri ve opsiyonel biberleme gibi işlemlerle parolanın güvenli bir kriptografik anahtara dönüştürülmesi açıklanmaktadır. Şekil, bu işlemin iç işleyişini görsel olarak ortaya koyarken, Tablo 3'te gösterilen çıktı değerleri ise bu süreçlerin depolama ve doğrulama amaçlı nasıl kodlandığını yansıtmaktadır.

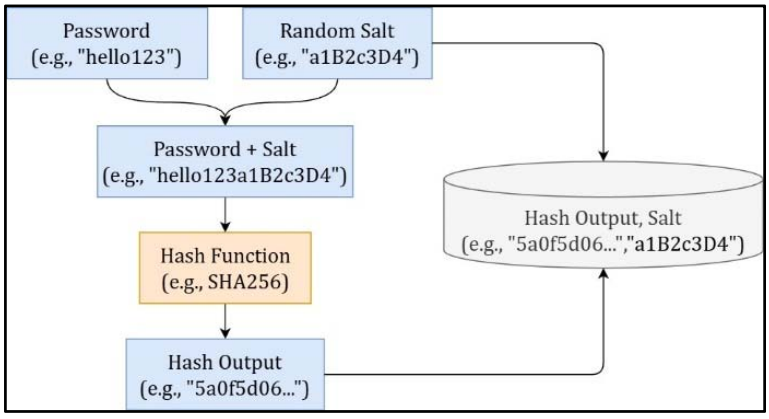
Algorithm 1 Key Derivation Function (KDF)

```
procedure KDF(password, salt, iterations, keyLength)
    hashOutput ← 0
    blockCount ← CEIL(keyLength/HashOutputSize)
    for i = 1 to blockCount do
        U ← HMAC(password, salt||IntToBytes(i))
        T ← U
        for j = 2 to iterations do
            U ← HMAC(password, U)
            T ← T ⊕ U
        end for
        hashOutput ← hashOutput||T
    end for
    return FIRSTkeyLengthBYTESOFhashOutput
end procedure
```

Şekil 3.1 Genel Bir KDF'nin Sahte Kod Uygulaması

3.3 TUZLAMA VE BİBERLEME İLE GÜVENLİĞİN ARTIRILMASI

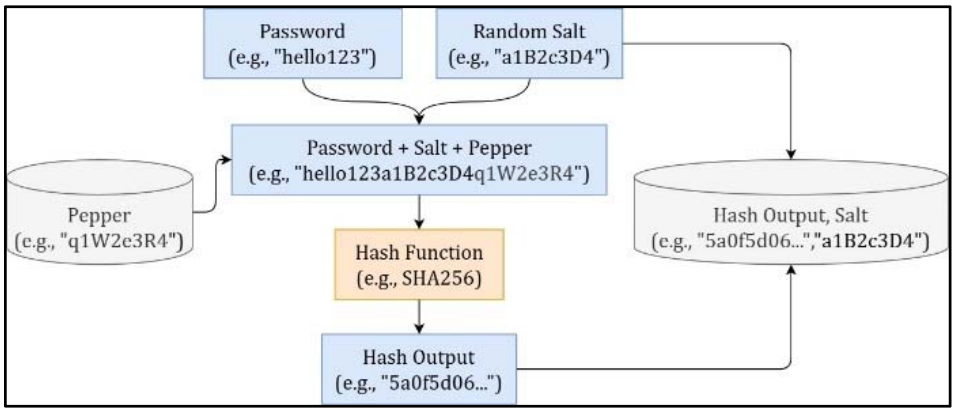
Aynı parolaların farklı karma çıktıları üretmesini sağlamak amacıyla tuzlama işlemi, parolaya rastgele bir değer eklenmesini içerir. Bu yöntem, önceden hesaplanmış karma değeri tabloları (ör. rainbow table) aracılığıyla yapılan saldırıları etkisiz hale getirerek, hesaplanmış durumdaki karma değeri karşılaştırmalarını geçersiz kılar (Bellovin ve Merritt, 1993). Şekil 2.2, kullanıcı parolasına tuzlama uygulanarak nasıl farklı karma çıktılarının elde edildiğini göstermektedir.



Şekil 3.2 Parola Karma İşleminde Tuz (Salt) Kullanma Süreci

ASVS v4.0.3 standardı, parola karma işlemlerinde KDF kullanılmasını ve çakışma riskini azaltmak amacıyla minimum 32 bit uzunluğunda tuz (salt) değerlerinin tercih edilmesini önermektedir (OWASP ASVS, 2021).

Öte yandan biberleme (peppering), veritabanında saklanmayan sistem genelinde gizli bir değerin parola üzerine eklenmesini içerir. Bu yöntem, önceden hesaplanmış saldırılara karşı direnci önemli ölçüde artırır. Tuzlar (salt) şifreleme sonrası veriyle birlikte saklanabilirken, biber (pepper) değerleri genellikle ayrı güvenli modüllerde veya donanım güvenlik modüllerinde (HSM) tutulur. Böylece karma veritabanı ele geçirilse dahi parolaların çözülmesi büyük oranda engellenir (Blocki ve Sridhar, 2016). Şekil 2.3, sisteme özgü bir biber (pepper) değerinin parola ile birlikte nasıl işlendiğini göstermektedir.



Şekil 3.3 Parola Karma İşleminde Biber (Pepper) Kullanım Süreci

Argon2, Catena (Forler vd., 2013), Lyra2 ve MAKWA (Pornin, 2015) gibi modern KDF'ler tuzlama (salting) mekanizmasını içsel olarak barındırmaktadır. Ancak biberleme (peppering), ek bir uygulama olarak entegre edilmelidir. Bu yöntem, çevrimdışı kaba kuvvet saldırılarına karşı fazladan bir güvenlik katmanı sağlar (Blocki ve Sridhar, 2016). Bir saldırgan karma veritabanını ele geçirse dahi, biber (pepper) kullanımı parolanın doğrudan çözülmesini engeller.

3.4 PAROLA KARMA YARIŞMASI

Parola Karma Yarışması (PHC), geleneksel parola tabanlı KDF'lerin güvenlik zafiyetlerine çözüm getirmek amacıyla ileri düzey ve güvenli parola karma algoritmalarını belirlemek için başlatılmış önemli bir girişimdir. 2013 yılında başlatılan yarışma, farklı uygulama senaryolarına uygunluk, güvenlik ve verimlilik açısından değerlendirilen 22 aday arasından 9 finalisti seçmiştir (Hatzivasilis vd., 2015).

PHC, kriptografi araştırmacılarına PBKDF2, bcrypt ve scrypt gibi geleneksel yöntemlerin ötesinde algoritmalar önermeleri, analiz etmeleri ve iyileştirmeleri için bir platform sağlamıştır. Yarışma sonucunda seçilen algoritmalar, bellek zorluğu yüksek yapıları sayesinde GPU, FPGA ve ASIC gibi donanım hızlandırmalı kaba kuvvet saldırılarına karşı güçlü direnç göstermiştir (Blocki vd., 2018).

PHC'nin temel odak noktası, bellek-zorlayıcı (memory-hard) yapıların teşvik edilmesidir. Bu yapıların amacı, saldırganın büyük miktarda RAM tüketmesini zorunlu hale getirerek paralel hesaplama tabanlı saldırıların etkisini azaltmaktır. PHC kazananı olan Argon2, bu özellikleriyle öne çıkmış ve daha sonra RFC 9106 (2021) standardı ile belgelendirilmiş, NIST tarafından önerilen parola karma fonksiyonu haline gelmiştir (Grassi vd., 2023).

PHC, bellek tüketimi, işlem süresi ve yan kanal saldırıları, kaba kuvvet denemeleri ve çöp toplayıcı (garbage collector) açıklarından etkilenebilirlik gibi çok sayıda parametrede empirik analizler sunmuştur. Bu sayede, hem güvenli hem de farklı ortamlarda uygulanabilir algoritmaların seçilmesi sağlanmıştır (örneğin: web kimlik doğrulama, gömülü sistemler, kriptografik anahtar yönetimi) (Hatzivasilis, 2017).

Tablo 3.1 KDF Özetleri (Github, 2025)

KDF	Digest
Argon	$argon2id$v=19$m=65536,t=2,p=1$gZiV/M1gPc22E$lH1En5eHEPvWWzApCTetd3Xl65ytiM4W99bRjFpbM
Battcrypt	Herkese açık olarak yayımlanmış bir özet formatı bulunmamaktadır
Catena	$catena$dragonfly10m=65536,t=2,p=1$ileG836J$pmSICYS8Nh8utulAeb5CztaWXtczijq0ZoJZqqHsL1T
Lyra2	$lyra2$1$m=65536,t=2,r=4$nIks49z6$CR2hYiziZcmBPOV56JisutRGt2txcS6iSHLLhrKvg6b
MAKWA	$makwa$2048,t=10000$2Ztq41qm$k9yoBQDf7NW9wVi4Q4saesgJyN386uWH7P3VbeMCfQU
Parallel	Herkese açık olarak yayımlanmış bir özet formatı bulunmamaktadır
POMELO	Herkese açık olarak yayımlanmış bir özet formatı bulunmamaktadır
Pufferfish	Herkese açık olarak yayımlanmış bir özet formatı bulunmamaktadır
yescrypt	yj9T$F5Jx5fExrKuPp53xLKQ..1$tVtFMx0Aj05nVcJZIUjztwvFLQncJjGsMPR6wV748pN

Yarışma, hibrit parola karma yaklaşımları ve adaptif maliyet parametreleri gibi yenilikçi yöntemleri tanıtarak, farklı güvenlik modellerine uyum sağlayabilen esnek çözümler geliştirilmesine olanak sağlamıştır (Hatzivasilis vd., 2015). Ayrıca, SHA-1 ve MD5 gibi klasik karma algoritmalarının güvenlik açıklarını ve PBKDF2, bcrypt ve scrypt gibi geleneksel KDF'lerin sınırlılıklarını gidermek amacıyla daha modern ve güvenli algoritmaların geliştirilmesini teşvik etmiştir (Wetzels, 2016).

3.5 BELLEK-ZORLAYICI FONKSİYONLAR VE ZAMAN-BELLEK DENGELEMESİ

Bellek-zorlayıcı fonksiyonlar (MHFs), yüksek miktarda bellek kullanımını zorunlu kılarak hesaplama maliyetini artıran kriptografik ilkelerdir. Bu sayede GPU, FPGA ve ASIC gibi paralel hesaplama destekli donanımlar kullanan saldırganlar için kaba kuvvet saldırıları ciddi ölçüde yavaşlatılır (Alwen vd., 2018).

Bu alandaki önde gelen örnekler arasında Argon2 ve yescrypt yer almaktadır. Bu algoritmalar, paralelleştirilebilir saldırılar ve bellek optimizasyonları gibi tehditlere karşı direnç sağlayacak şekilde tasarlanmıştır. Bu fonksiyonlar, yüksek bellek bant genişliği gereksinimiyle paralel kaba kuvvet saldırılarını etkisiz hale getirir (Choe vd., 2019).

Zaman-bellek dengelemesi kavramı, parola karma süreçlerinde işlem süresi ile bellek kullanımı arasında bir denge kurmayı ifade eder. Bellek gereksinimlerinin artırılması, kaba kuvvet saldırılarını daha maliyetli hale getirerek uygulanabilirliğini azaltır (Luo vd., 2021). Ancak, bu tür fonksiyonların gerçek sistemlerde uygulanması sırasında özellikle düşük güçlü gömülü cihazlar ve bulut tabanlı platformlar gibi kaynak kısıtlı ortamlarda dikkatli bir planlama gerektirir.

3.6 KUANTUM SONRASI KRİPTOGRAFİ VE ANAHTAR TÜRETME FONKSİYONLARI

Kuantum hesaplama, özellikle geleneksel KDF'lerin güvenliğini ciddi şekilde tehdit etmektedir. Grover'ın algoritması, klasik bilgisayarlara göre kuantum bilgisayarların sırasız veritabanlarını karekök hızında taramasına imkan tanır; bu da simetrik kriptografik sistemlerin güvenliğini zayıflatır (Grover, 1996). Shor'un algoritması ise büyük sayıları çarpanlarına ayırabilmekte ve ayrık logaritmaların hesaplanmasını sağlayarak RSA ve ECC gibi asimetrik şemaları etkisiz hale getirmektedir (Shor, 1994).

Moore Yasası, bir entegre devredeki transistör sayısının yaklaşık her 18 ayda iki katına çıktığını öngörür (Moore, 1965). Başlangıçta klasik bilgi işlem için geçerli olan bu öngörü, artık kuantum donanımında da benzer hızlarda ilerlemelerle gözlemlenmektedir. Qubit stabilitesi ve hata düzeltme tekniklerindeki gelişmeler sayesinde, önümüzdeki yirmi yıl içinde RSA-2048 veya ECC-256 gibi sistemlerin kırılabilir hale gelmesi olasıdır (Grassi vd., 2023).

Bu riskleri azaltmak için, kuantum kaba kuvvet saldırılarına karşı dirençli kuantum sonrası KDF'lerin geliştirilmesi gereklidir. Simetrik kriptografi teknik olarak anahtar uzunluklarını iki katına çıkararak Grover algoritmasına karşı korunabilir; ancak bu çözüm, donanım gelişmeleri karşısında geçici bir önlemdir. PHC finalistlerinden Argon2 ve yescrypt, bellek-zorlayıcı yapıları sayesinde kuantum saldırılarına karşı dayanıklılık göstermektedir. Bu algoritmalar, kuantum tabanlı kaba kuvvet saldırılarının uygulanabilirliğini pratikte imkansız hale getirir (Choe vd., 2019).

Kuantum teknolojisinin Moore Yasası hızında gelişmesiyle birlikte, kriptografik sistemlerin kuantum dirençli karma ve anahtar türetme tekniklerini benimsemesi zorunlu hale gelmektedir.

BÖLÜM 4

4. STANDARTLAŞMA VE REGÜLASYON UYUMU

Çeşitli regülasyon çerçeveleri, parola karma, kimlik doğrulama ve kriptografik anahtar yönetimi için standartlar belirlemektedir. Bu bölüm, parola karma uygulamalarını etkileyen mevcut güvenlik standartlarını ve düzenleyici gereklilikleri özetlemektedir.

4.1 PAROLA SAKLAMA İÇİN KRİPTOGRAFİK STANDARTLAR

Modern kriptografik önlemler, parolaların güvenli biçimde saklanmasını ve güçlü kimlik doğrulama protokollerinin uygulanmasını temel alır. Aşağıda dikkate alınması gereken başlıca yönergeler yer almaktadır:

- NIST SP 800-63B: Kaba kuvvet ve çevrimdışı saldırılara karşı dayanıklı parola karma tekniklerini önermektedir. Bu tür saldırıların maliyetini artırmak için bellek-zorlayıcı bir KDF'in kullanılması tavsiye edilmektedir. Minimum 32 bit tuz (salt) uzunluğu gerekliliğine ek olarak, NIST, tuzların pratikte en az 112 bit entropi sağlaması gerektiğini vurgular. Bu ayrım, tuz (salt) uzunluğu ile entropinin aynı kavramlar olmadığını ortaya koyar; tuz'ların (salt) tahmin edilemezlik ve çakışma direnci sağlamak adına kriptografik olarak güvenli sahte rastgele sayı üreteçleri (CSPRNG) ile oluşturulması gerekmektedir (Grassi vd., 2023).
- ISO/IEC 27001: Kuruluşların bilgi varlıklarının (örneğin kimlik bilgileri ve kimlik doğrulama mekanizmaları) gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak amacıyla uygun örgütsel, insan kaynaklı, fiziksel ve teknolojik kontrolleri uygulamasını zorunlu kılar. Bilgi Güvenliği Yönetim Sistemi (BGYS) çerçevesinde, güvenli parola politikalarının hayata geçirilmesini ister; bu da korumalı depolama, erişim sınırlamaları ve kimlik doğrulama kontrollerinin düzenli olarak gözden

geçirilmesini kapsar. ISO/IEC 27001 belirli kriptografik teknikler tanımlamasa da, parola verilerinin korunması için sektör standardı olan KDF'lerin, güvenli karma fonksiyonlarının ve tuzlama (salting) mekanizmalarının kullanılmasını güçlü biçimde tavsiye eder. Özellikle ISO/IEC 27001:2022'nin Ek A bölümünde yer alan Kontrol A.9.4.3 – Parola Yönetim Sistemi, güçlü, öngörülemez ve güvenli biçimde saklanan parolaların kullanımını zorunlu kılar (ISO/IEC 27001: 2022, 2022).

- PCI DSS: Kart sahibi verilerini işleyen, depolayan veya ileten kuruluşların, kullanıcı parolaları dahil olmak üzere kimlik bilgilerini güvence altına almak için güçlü kriptografi uygulamasını gerektirir. Saklanan parolalar, tuz (salt) değeri ile birlikte güçlü tek yönlü karma algoritmaları kullanılarak okunamaz hale getirilmelidir ve bu süreç tanınmış kriptografik standartlara uygun olarak uygulanmalıdır. PCI DSS belirli bir algoritma dayatmasa da, HMAC veya sektör onaylı KDF'lerin kullanımını önermekte ve elde edilen kriptografik gücün en az 128 bit güvenlik seviyesine eşdeğer olmasını şart koşmaktadır. Ayrıca, parolaların en az 90 günde bir değiştirilmesi ve ödeme verilerini işleyen sistemlerde yönetsel erişim için çok faktörlü kimlik doğrulama (MFA) kullanılması zorunludur (Industry, 2024).
- OWASP Uygulama Güvenliği Doğrulama Standardı (ASVS): OWASP ASVS, sistemlerin gelişen saldırı tekniklerine karşı hesaplama maliyetlerini uyarlayabilmesini sağlayan adaptif güvenlik özelliklerini destekleyen parola karma uygulamalarını savunur. ASVS v4.0.3, parola karma için bir KDF'in kullanımını ve çakışma riskini azaltmak amacıyla minimum 32 bit tuz (salt) uzunluğunun tercih edilmesini önerir. PBKDF2 kullanılıyorsa, yineleme sayısı en az 100.000 olmalıdır. bcrypt için ise önerilen iş faktörü en az 13'tür. Ancak bu sürümde PHC finalistlerine yer verilmemiştir (OWASP ASVS, 2021). Yaklaşan ASVS v5.0 ("Bleeding Edge") ise PHC'nin kazananı olan Argon2'yi önerilen algoritma olarak tanıtır. Spesifik olarak, Argon2id yapılandırması için 19 MB bellek maliyeti, 2 zaman maliyeti ve 1 paralellik faktörü önerilir.

PBKDF2_SHA512 algoritması için 210.000 yineleme gerekirken, FIPS-140 uyumluluğu için önerilen PBKDF2_SHA256 algoritması 600.000 yineleme içermelidir. Yeni sürüm ayrıca, Argon2id mevcut olmadığında alternatif olarak scrypt algoritmasını sunar; burada 2^{1} maliyet parametresi, minimum 8 blok boyutu ve 1 paralelleştirme parametresi gereklidir. bcrypt'e yönelik öneriler ise değişmemiştir ve bu algoritma eski sistemler için uygun görülmektedir (OWASP ASVS, 2025).

Bu standartlar, tuzlama (salting), anahtar uzatma (key stretching) ve bellek-zorlayıcı fonksiyonlar (MHFs) gibi uygulamaları teşvik ederek parola tahminine dayalı saldırıların önlenmesini ve kriptografik en iyi uygulamaların benimsenmesini hedeflemektedir.

4.2 VERİ KORUMA REGÜLASYONLARI VE KRİPTOGRAFİK BEKLENTİLER

Her ne kadar mevcut yasal düzenlemeler KDF kullanımını açıkça zorunlu kılmasa da, modern gizlilik yasaları kriptografik olarak güvenli parola işleme tekniklerini güçlü şekilde tavsiye etmektedir. Bu bağlamda, Argon2 gibi gelişmiş KDF'lerin veya kullanılabilirlik durumuna göre bcrypt, PBKDF2 ve scrypt gibi geleneksel alternatiflerin kullanılması önerilmektedir.

Kuruluşların yüksek entropili, bellek-zorlayıcı ve hesaplama açısından uyarlanabilir KDF'ler uygulaması, yerleşik güvenlik en iyi uygulamalarıyla uyumluluk açısından beklenen bir yükümlülüktür. Örneğin, GDPR Madde 32, kişisel verilerin korunması için uygun teknik ve organizasyonel önlemlerin (TOM) alınmasını şart koşar. Her ne kadar spesifik algoritmalar belirtilmese de, bu madde güçlü şifreleme ve karma mekanizmalarının dolaylı olarak kullanımını zorunlu kılar (GDPR, 2016).

Benzer biçimde, CCPA, LGPD, PIPL, PIPEDA ve KVKK gibi küresel veri koruma düzenlemeleri, güvenli veri işleme yükümlülüğünü vurgular. Bu çerçeveler, ihlaller karşısında yasal yaptırımlar uygulamakta ve hassas verilerin

korunması için güncel kriptografik tekniklerin kullanılmasını tavsiye etmektedir (KVKK, 2016; CCPA, 2018; LGPD, 2018; PIPEDA, 2000; PIPL, 2021).

PHC finalistleri arasında, Argon2, sağlam güvenlik özellikleri, bellek-zorlayıcı yapısı ve çağdaş kriptografik normlarla uyumluluğu nedeniyle en çok tercih edilen algoritmadır. Her ne kadar resmi regülasyonlar bu algoritmanın kullanımını zorunlu tutmasa da, Argon2 güncel kriptografik standartlara uyum sağlayan üstünlüğü nedeniyle öne çıkmaktadır.

BÖLÜM 5

5. BULGULAR

Bu bölümde, PHC finalistlerinin çok boyutlu bir değerlendirmesi sunulmaktadır. Değerlendirme; performans ölçütleri, güvenlik analizleri ve mevcut kriptografik standartlar ile gizlilik düzenlemeleriyle uyumluluk haritası üzerinden yapılmıştır.

5.1 PERFORMANS ANALİZİ

Tablo 5.1'de sunulan PHC finalistlerinin performans karşılaştırması, uygulama süresi, bellek kullanımı ve kod boyutu bakımından önemli farklılıkları ortaya koymaktadır.

Uygulama süresi açısından en hızlı algoritma 0,015621 ms ile MAKWA olurken, onu Parallel (0,047051 ms) ve yescrypt (0,058253 ms) takip etmektedir. Buna karşın, Argon ve Pufferfish daha yüksek uygulama sürelerine sahiptir; bu da güvenlik özellikleri ile hesaplama verimliliği arasında bir ödünleşimi işaret etmektedir.

Bellek kullanımı da önemli bir etkendir. POMELO, 1KB ile 8GB arasında değişen kullanımıyla en geniş aralığa sahiptir ve bu durum onu oldukça esnek fakat potansiyel olarak kaynak tüketici bir seçenek haline getirir. Benzer şekilde, Argon ve Lyra2 de 1GB'a kadar bellek gerektirebilir ve bu, bellek kısıtlı ortamlarda dezavantaj teşkil edebilir. Buna karşın, Parallel algoritması ihmal edilebilir düzeyde bellek kullanırken, MAKWA ve yescrypt orta düzeyde kaynak tüketimine sahiptir.

Kod boyutu açısından ise Pufferfish 103KB ile en büyük yer kaplayan algoritma iken, onu Lyra2 (98KB) ve MAKWA (95KB) izlemektedir. Bu da daha karmaşık uygulamaları işaret eder. Öte yandan, Catena (25KB) ve battcrypt (27KB) en hafif çözümler arasında yer almaktadır.

Genel olarak, uygun bir PHC finalisti seçimi; güvenlik, hesaplama verimliliği ve sistem kaynaklarının dengeli kullanımı arasında yapılacak tercihlere bağlıdır. Argon ve POMELO gibi bellek-zor fonksiyonlar (MHF) yüksek güvenlik sağlarken, önemli bellek yükü oluşturarak sınırlı ortamlarda kullanımını kısıtlayabilir. Buna karşılık, MAKWA ve Parallel gibi hafif çözümler yüksek hız ve düşük kaynak kullanımı sunar ancak yüksek güvenlikli sistemlerde ek kriptografik doğrulama ve yan kanal koruması gerektirebilir.

Tablo 5.1 PHC Finalistlerinin Performans Karşılaştırması (Forler vd., 2013; Simplicio vd., 2014; Thomas, 2014; Gosney, 2015; Hatzivasilis vd., 2015; Peslyak, 2015; Pornin, 2015; Thomas, 2015; Wu, 2015; RFC 9106, 2021).

KDF	Yürütme(Execution) Süresi (ms) MIN-MAX	Bellek Kullanımı (KB)	Kod Boyutu (KB)
Argon	0,008917 - 577.02208	1KB - 1GB	82
Battcrypt	0,000312 - 2.853051	18KB - 128MB	27
Catena	0,353742 - 5.461030	8MB	25
Lyra2	0,000084 - 2.916398	400MB - 1GB	98
MAKWA	0,000096 - 0.015621	335KB	95
Parallel	0,001000 - 0.047051	-	71
POMELO	0,000031 - 8.504152	1KB - 8GB	67
Pufferfish	0,000057 - 38.341005	4KB - 16KB	103
yescrypt	0,000094 - 0.058253	44KB - 3MB (RAM), 3GB (ROM)	36

5.2 GÜVENLİK ANALİZİ

Tablo 5.2, PHC finalistlerinin güvenlik açısından karşılaştırmasını sunmakta; GPU tabanlı saldırılara direnç, bellek zorluluğu (MH), yan kanal

direnci (SCR) ve öngörülemezlik (PR) gibi güvenlik özelliklerini değerlendirmektedir.

GPU direnci, saldırganların kaba kuvvet saldırılarını paralel hale getirme kabiliyetine karşı önemli bir savunma unsurudur. Argon, battcrypt, Catena, Lyra2, POMELO ve Pufferfish gibi finalistler GPU direncine sahiptir ve bu sayede donanım tabanlı saldırılara karşı güçlü bir savunma sunar. Buna karşın, MAKWA, Parallel ve yescrypt bu dirence sahip değildir ve özel donanım kullanılarak yapılan saldırılara karşı daha savunmasız olabilir.

MH özelliği, özellikle parola kırma gibi saldırılarda karşı tarafın hesaplama yükünü artırarak etkili bir koruma sağlar. Argon, battcrypt, Catena, Lyra2 ve POMELO gibi algoritmalar bellek-zorlu yapılarıyla bu beklentiyi karşılar. Ancak MAKWA ve Parallel bu özelliğe sahip değildir. yescrypt ise belleğe erişimde ROM tabanlı ardışık bir yaklaşım benimseyerek farklı bir yapı sunar.

Yan kanal direnci (SCR) ise algoritmaların güç tüketimi, elektromanyetik yayılım veya zamanlama farkları gibi bilgiler üzerinden yapılacak saldırılara karşı korunmasını sağlar. Catena ve Parallel, özellikle yan kanal saldırılarına karşı dayanıklı olacak şekilde tasarlanmıştır. Argon ise, Argon2i varyantı ile bu yönde bir koruma sunar. MAKWA ve POMELO ise sınırlı yan kanal direncine sahiptir. battcrypt, Lyra2 ve Pufferfish gibi finalistler için ise bu konuda belgelenmiş bir koruma bulunmamaktadır.

Sonuç olarak, PHC finalistlerinin sunduğu güvenlik özellikleri farklılaşmakta; bazı algoritmalar GPU direnci ve bellek-zorluğu üzerinde yoğunlaşırken, diğerleri yan kanal saldırılarına karşı koruma sağlamayı hedeflemektedir. Uygun KDF seçimi, uygulamanın güvenlik gereksinimlerine göre belirlenmelidir ve kaba kuvvet, yan kanal ve öngörülemezlik saldırılarına karşı direnç ile operasyonel verimlilik ve uygulanabilirlik dengelenmelidir.

Tablo 5.2 PHC Finalistlerinin Güvenlik Karşılaştırması (Simplicio vd., 2014; Thomas, 2014; Forler vd., 2015; Gosney, 2015; Hatzivasilis vd., 2015; Peslyak, 2015; Pornin, 2015; Thomas, 2015; Wu, 2015; RFC 9106, 2021).

Fonksiyon	GPU Direnci	Bellek-Zorluk	Yan kanal direnci
Argon	✓	✓	Argon2i
Battcrypt	✓	✓	-
Catena	✓	✓	✓
Lyra2	✓	✓	-
MAKWA	-	-	Kısmen
Parallel	-	-	✓
POMELO	✓	✓	Kısmen
Pufferfish	✓	✓	-
yescrypt	-	ROM-Port, sequential	-

5.3 UYUMLULUK ANALİZİ

Parola karma mekanizmalarının güvenlik standartları ve gizlilik düzenlemeleriyle uyumlu olması, değerlendirme sürecinde kritik bir rol oynamaktadır. Bu bölümde, PHC finalistlerinin temel güvenlik standartları ve gizlilik mevzuatlarıyla olan uyumu kapsamlı şekilde incelenmektedir.

NIST SP 800-63B, parola temelli kimlik doğrulama için dijital kimlik rehberleri sunmakta ve tuzlanmış karma fonksiyonların kullanımını, sözlük saldırılarına karşı dirençli yapıları ve zayıf parola kurallarından kaçınılmasını önermektedir. Argon2 gibi PHC finalistleri, bellek zorlayıcı fonksiyonlar kullanarak kaba kuvvet ve GPU saldırılarına karşı direnç sağladığı için bu ilkelerle uyumludur (Grassi et al., 2023).

ISO/IEC 27001 standardı, bir bilgi güvenliği yönetim sistemi (ISMS) oluşturulmasını gerektirir. Bu da güçlü kriptografik kontrollerin benimsenmesini

zorunlu kılar. PHC finalistleri, anahtar genişletme (key stretching) ve güvenli KDF yapılarını içermeleriyle bu gereklilikleri karşılamaktadır (ISO/IEC 27001:2022, 2022).

PCI DSS, ödeme sistemlerinde güvenli kimlik doğrulama ve parola depolama mekanizmalarını zorunlu kılar. Kullanılan algoritmaların öngörülemezliğe ve kaba kuvvet saldırılarına dirençli olması gerekir. Özellikle Argon2 ve Lyra2 bu korumayı sundukları için PCI DSS ile uyum göstermektedir (Industry, 2024).

OWASP ASVS 4.0.3, güvenli yazılım geliştirme için rehberlik sunmakta ve güçlü kimlik doğrulama ile parola depolama mekanizmalarına odaklanmaktadır. Uyarlanabilir, bellek-zorlu algoritmaların kullanımı önerilmektedir ki bu gereklilikler PHC finalistleri tarafından genel olarak karşılanmaktadır (OWASP ASVS, 2021).

GDPR, kişisel verilerin yetkisiz erişime karşı korunması için güçlü teknik önlemler öngörür. 32. Madde, şifreleme ve takma adlandırma gibi tekniklerin kullanımını zorunlu kılar. Güçlü parola karma algoritmaları bu gereklilikle örtüşmektedir (GDPR, 2016).

CCPA, Kaliforniya sakinlerinin kişisel verilerini korumayı amaçlamakta olup, veri ihlallerini önleyecek "makul güvenlik önlemleri"nin alınmasını öngörür. PHC finalistlerinin uygulanması bu çerçevede uyumluluk sağlar (CCPA, 2018).

Brezilya'nın LGPD yasası da benzer şekilde teknik ve idari veri koruma önlemleri öngörmektedir. Kaba kuvvet saldırılarına ve kimlik bilgisi sızıntılarına karşı koruma sunan parola karma teknikleri bu düzenleme ile uyumludur (LGPD, 2018).

Çin'in PIPL düzenlemesi, kişisel verilerin güvenli şekilde işlenmesini ve şifreleme ile veri minimizasyonunu ön planda tutar. PHC finalistleri bu gereklilikleri karşılamaktadır (PIPL, 2021).

Kanada'nın PIPEDA düzenlemesi, hassas verilerin korunması için uygun güvenlik önlemleri alınmasını şart koşar. Güvenli parola depolama sağlayan PHC finalistleri bu beklentileri karşılamaktadır (PIPEDA, 2000).

Türkiye'nin KVKK düzenlemesi de GDPR ile benzer ilkeleri benimser ve kişisel verilerin korunmasında yeterli teknik ve idari önlemlerin alınmasını zorunlu kılar. PHC finalistlerinin kullanımı, güçlü parola koruma teknikleri sayesinde KVKK uyumluluğunu sağlar (KVKK, 2016).

Genel olarak, PHC finalistleri; önemli güvenlik standartları ve gizlilik düzenlemeleri ile yüksek düzeyde uyumluluk sergilemektedir. Bu algoritmaların kimlik doğrulama sistemlerinde uygulanması, modern tehditlere karşı direnç sağlar ve düzenleyici gerekliliklerin karşılanmasına katkıda bulunur. Bu uyumluluk hem veri ihlali risklerini hem de yasal sorumlulukları azaltmada etkili olmaktadır.

Tablo 25.3'te, PHC finalistlerinin başlıca küresel kriptografik standartlar ve veri koruma düzenlemeleriyle olan uyumları karşılaştırmalı olarak sunulmuştur.

PCI DSS ve NIST SP 800-63B standartlarının kriptografik gereklilikleri; bellek zorlayıcı fonksiyonlar olarak tasarlanmış ve kapsamlı güvenlik analizinden geçmiş Argon2, Catena ve Lyra2 ile örtüşmektedir. Ayrıca, yaklaşan OWASP ASVS v5.0.0 sürümünde Argon2 açıkça önerilen bir KDF olarak yer almaktadır. ISO/IEC 27001 standardı ile GDPR, KVKK, LGPD ve PIPL gibi gizlilik odaklı düzenlemeler de güçlü kriptografik karma mekanizmalarını zorunlu kılmaktadır. Bu gereksinimler, Argon2, Catena, Lyra2, MAKWA ve yescrypt tarafından sağlanan güçlü güvenlik özellikleriyle karşılanmaktadır.

Tablo 5.3 Uyumluluk Haritalaması: PHC Finalistleri ve Küresel Kriptografik Standartlar

Düzenleme	**Kriptografik Gereksinim**	**PHC Uyumlaştırması**
GDPR	Teknik ve organizasyonel önlemler (Article 32)	Argon2, Catena, Lyra2, MAKWA, yescrypt
ISO/IEC 27001	ISMS'de güvenli kimlik bilgisi işleme	Argon2, Catena, Lyra2, MAKWA, yescrypt

Tablo 5.3 (Devamı) Uyumluluk Haritalaması: PHC Finalistleri ve Küresel Kriptografik Standartlar

Düzenleme	**Kriptografik Gereksinim**	**PHC Uyumlaştırması**
PCI DSS	Tek yönlü karma, 128 bitlik güç	Argon2, Catena, Lyra2
OWASP ASVS	Uyarlanabilir, bellek-zor KDF'ler	Argon2
KVKK, LGPD, PIPL	Güçlü şifreleme ve karma	Argon2, Catena, Lyra2, MAKWA, yescrypt
LGPD	Güçlü şifreleme ve karma	Argon2, Catena, Lyra2, MAKWA, yescrypt
PIPL	Güçlü şifreleme ve karma	Argon2, Catena, Lyra2, MAKWA, yescrypt
NIST SP 800-63B	Tuzlama, MHF'ler, entropi	Argon2, Catena, Lyra2

SONUÇ VE ÖNERİLER

Bu çalışma, PHC finalistleri arasında Argon2'nin özellikle bellek-zorlayıcı (memory-hard) tasarımı sayesinde donanım hızlandırmalı kaba kuvvet saldırılarına karşı dayanıklılığıyla en güvenli ve en etkili modern anahtar türetme fonksiyonu (KDF) olarak öne çıktığını ortaya koymaktadır (Choe vd., 2019). Bcrypt, uzun vadeli destek ve geriye dönük uyumluluğa ihtiyaç duyan eski sistemler için geçerli bir seçenek olmaya devam ederken, yescrypt, genel amaçlı ortamlarda kullanılabilecek güvenlik-performans dengesi sunmaktadır. Algoritma seçimi, sistemin güvenlik gereksinimleri ve kaynak kısıtlarına göre uyarlanmalıdır.

Argon2, kaba kuvvet ve paralel saldırılara karşı yüksek direnç gösterdiği için web uygulamaları açısından da önerilen bir şifreleme algoritmasıdır. Argon2'nin uygun bellek ve zaman parametreleriyle yapılandırılması, geniş çaplı saldırılara karşı güçlü bir koruma sağlar. Ayrıca, tuz (salt) ve biber (pepper) mekanizmalarının kullanımı güvenliği daha da artırmaktadır.

Sınırlı işlem gücü ve bellek kaynaklarına sahip gömülü sistemler ve Nesnelerin İnterneti (IoT) uygulamaları için ise bcrypt ve scrypt, düşük kaynak gereksinimleri sayesinde kabul edilebilir çözümler sunmaktadır. Aynı zamanda, Argon2'nin bellek parametreleri ayarlanarak bu ortamlarda da yüksek güvenlik, makul kaynak kullanımı ile sağlanabilir.

NIST SP 800-63B, ISO/IEC 27001 ve PCI DSS gibi standartlar belirli KDF'leri zorunlu kılmasa da; bellek-zorlayıcılığı, entropi ve tek yönlü fonksiyon kullanımı gibi temel gereksinimleri vurgulamaktadır. Buna karşılık OWASP ASVS, Argon2'yi ismen ve belirli yapılandırma parametreleriyle birlikte önermektedir. Bu, parola karma konusunda en iyi uygulamalar için yön gösterici kuralların daha belirleyici hale geldiğini göstermektedir (OWASP ASVS, 2025).

Sonuç olarak, gelecekteki araştırmaların, hem verimli hem de uyarlanabilir olmasının yanı sıra formel olarak doğrulanmış ve kuantuma dayanıklı parola karmalama algoritmalarının geliştirilmesine odaklanması gerekmektedir.

Özellikle özel donanımlar ve kuantum hesaplama gibi yeni saldırı vektörlerinin ortaya çıkmasıyla birlikte, dijital kimlik doğrulama ekosistemlerinin korunması için sürekli kriptografik yenilik hayati önem taşımaktadır.

KAYNAKLAR

Álvarez, R., & Zamora, A. (2017). Using spritz as a password-based key derivation function. In *International Joint Conference SOCO'16-CISIS'16-ICEUTE'16: San Sebastián, Spain, October 19th-21st, 2016 Proceedings 11* (pp. 518-525). Springer International Publishing.

Alwen, J., Gazi, P., Kamath, C., Klein, K., Osang, G., Pietrzak, K., ... & Rybár, M. (2018, May). On the memory-hardness of data-independent password-hashing functions. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security* (pp. 51-65).

Andrade, E. R., Simplicio, M. A., Barreto, P. S., & dos Santos, P. C. (2016). Lyra2: Efficient password hashing with high security against time-memory trade-offs. *IEEE Transactions on Computers*, *65*(10), 3096-3108.

Aumasson, J. P. (2013). Password Hashing: the Future is Now.

Bellovin, S. M., & Merritt, M. (1993, December). Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise. In *Proceedings of the 1st ACM Conference on Computer and Communications Security* (pp. 244-250).

Blocki, J., & Sridhar, A. (2016, May). Client-cash: Protecting master passwords against offline attacks. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security* (pp. 165-176).

Blocki, J., Harsha, B., & Zhou, S. (2018, May). On the economics of offline password cracking. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 853-871). IEEE.

CCPA. 2018. California Consumer Privacy Act (CCPA). URL: https://oag.ca.gov/privacy/ccpa (accessed date: March 04, 2025).

Choe, J., Moreshet, T., Bahar, R. I., & Herlihy, M. (2019, September). Attacking memory-hard scrypt with near-data-processing. In *Proceedings of the International Symposium on Memory Systems* (pp. 33-37).

Clark, M., & Seamons, K. (2022, October). Passwords and Cryptwords: The Final Limits on Lengths. In *Proceedings of the 2022 New Security Paradigms Workshop* (pp. 75-89).

Forler, C., List, E., Lucks, S., & Wenzel, J. (2014, December). Overview of the Candidates for the Password Hashing Competition: And Their Resistance Against Garbage-Collector Attacks. In *International Conference on Passwords* (pp. 3-18). Cham: Springer International Publishing.

Forler, C., Lucks, S., & Wenzel, J. (2013). Catena: A memory-consuming password-scrambling framework. *Cryptology ePrint Archive*.

GDPR. 2016. General Data Protection Regulation (GPDR). URL: https://gdpr-info.eu/ (accessed date: March 04, 2025).

Gosney J. 2015. Pufferfish2 password hashing scheme. URL: https://github.com/epixoip/pufferfish (accessed date: April 04, 2025).

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., ... & Theofanos, M. F. (2016). Draft nist special publication 800-63b digital identity guidelines. *National Institute of Standards and Technology (NIST)*, *27*.

Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 212-219).

Hatzivasilis, G. (2017). Password-hashing status. *Cryptography*, *1*(2), 10.

Hatzivasilis, G., Papaefstathiou, I., & Manifavas, C. (2015). Password hashing competition-survey and benchmark. *Cryptology ePrint Archive*.

Industry PC. 2024. Data security standard. Requirements and Security Assessment version, 4.0.1. URL: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf (accessed date: March 04, 2025).

ISO/IEC 27001: 2022. 2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/27001 (accessed date: March 04, 2025).

Kodwani, G., Arora, S., & Atrey, P. K. (2021, July). On security of key derivation functions in password-based cryptography. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 109-114). IEEE.

KVKK. 2016. Personal Data Protection Law (KVKK). URL: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5 (accessed date: March 04, 2025).

Lata, K., & Bansal, A. (2021, December). Timing side-channel attack resistant key derivation functions for cryptosystems. In *2021 IEEE International Symposium on Smart Electronic Systems (iSES)* (pp. 395-399). IEEE.

LGPD. 2018. General Personal Data Protection Law (LGPD). URL: https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf (accessed date: March 04, 2025).

Lu, Y. F., Kuo, C. F., & Fang, Y. Y. (2016, October). Efficient storage encryption for android mobile devices. In *Proceedings of the International Conference on Research in Adaptive and Convergent Systems* (pp. 213-218).

Luo, Y., Su, Z., Zheng, W., Chen, Z., Wang, F., Zhang, Z., & Chen, J. (2021). A novel memory-hard password hashing scheme for blockchain-based cyber-physical systems. *ACM Transactions on Internet Technology (TOIT)*, *21*(2), 1-21.

Mcginthy, J. M., & Michaels, A. J. (2019). Further analysis of PRNG-based key derivation functions. *IEEE Access*, *7*, 95978-95986.

Moore, G. E. (2006). Cramming more components onto integrated circuits, Reprinted from Electronics, volume 38, number 8, April 19, 1965, pp. 114 ff. *IEEE solid-state circuits society newsletter*, *11*(3), 33-35.

OWASP ASVS. 2021. Open Worldwide Application Security Project Application Security Verification Standard (OWASP ASVS) v4.0.3. URL: https://github.com/OWASP/ASVS/blob/master/4.0/en/0x11-V2-Authentication.md (accessed date: March 04, 2025).

OWASP ASVS. 2025. Open Worldwide Application Security Project Application Security Verification Standard (OWASP ASVS) v5.0. URL: https://github.com/OWASP/ASVS/blob/master/5.0/en/0x97-Appendix-V_Cryptography.md (accessed date: March 04, 2025).

OWASP Password Storage Cheat Sheet. 2025. URL: https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html#upgrading-the-work-factor (accessed date: March 23, 2025).

Peslyak A. 2015. yescrypt - a Password Hashing Competition submission. URL: https://www.password-hashing.net/submissions/specs/yescrypt-v2.pdf (accessed date: April 04, 2025).

PIPEDA. 2000. Personal information protection and electronic documents act. Department of Justice (PIPEDA). URL: http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf (accessed date: March 04, 2025).

PIPL. 2021. Personal Information Protection Law of the People's Republic of China (PIPL). URL: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (accessed date: March 04, 2025).

Pornin T. 2015. The MAKWA Password Hashing Function Specifications v1.1. URL: https://www.bolet.org/makwa/makwa-spec-20150422.pdf (accessed date: April 04, 2025).

Provos, N., & Mazieres, D. (1999, June). A future-adaptive password scheme. In *Proceedings of the annual conference on USENIX Annual Technical Conference* (pp. 32-32).

RFC 6070. 2011. PKCS #5: Password-Based Key Derivation Function 2 (PBKDF2) Test Vectors. URL: https://www.rfc-editor.org/info/rfc6070 (accessed date: April 2, 2025).

RFC 9106. 2021. Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications. URL: https://www.rfc-editor.org/info/rfc9106 (accessed date: March 20, 2025).

Saad, M. I. M., Jalil, K. A., & Manaf, M. (2016). Secured authentication using anonymity and password-based key derivation function. In *Mobile Web and Intelligent Information Systems: 13th International Conference, MobiWIS 2016, Vienna, Austria, August 22-24, 2016, Proceedings 13* (pp. 184-197). Springer International Publishing.

Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science* (pp. 124-134). Ieee.

Simplicio Jr, M. A., Almeida, L. C., Andrade, E. R., dos Santos, P. C., & Barreto, P. S. (2014). The Lyra2 reference guide. *Tech. Report v2. 3.2*.

Thomas S. 2014. Battcrypt. URL: https://www.password-hashing.net/submissions/specs/battcrypt-v0.pdf (accessed date: April 04, 2025).

Thomas S. 2015. Parallel. URL: https://www.password-hashing.net/submissions/specs/Parallel-v1.pdf (accessed date: April 04, 2025).

Tran, D. N., Nguyen Tien, X., Nguyen Xuan, T., & Le Viet, P. (2024, March). A User-Centric Key Management for Cloud Encryption Using Key Derivation Function. In *The International Conference on Intelligent Systems & Networks* (pp. 479-487). Singapore: Springer Nature Singapore.

URL-1. PHC string format. URL: https://github.com/P-H-C/phc-string-format/blob/master/phc-sf-spec.md (accessed date: April 1, 2025).

Wang, M., Duan, M., & Zhu, J. (2018, May). Research on the security criteria of hash functions in the blockchain. In *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts* (pp. 47-55).

Wetzels, J. (2016). Open sesame: The password hashing competition and Argon2. *arXiv preprint arXiv:1602.03097*.

Wu H. 2015. POMELO A Password Hashing Algorithm (Version 2). URL: https://www.password-hashing.net/submissions/specs/POMELO-v3.pdf (accessed date: April 04, 2025).

Yao, F. F., & Yin, Y. L. (2005). Design and analysis of password-based key derivation functions. In *Topics in Cryptology–CT-RSA 2005: The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005. Proceedings* (pp. 245-261). Springer Berlin Heidelberg.

Zhou, J., Chen, J., Pan, K., Zhao, C., & Li, X. (2012, August). On the security of key derivation functions in office. In *Anti-counterfeiting, Security, and Identification* (pp. 1-5). IEEE.

ÖZGEÇMİŞ