T.C
MALTEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
YÜKSEK LİSANS TEZİ

ELEKTRONİK OY VE UYGULAMALARI

Hazırlayan
Fatih SÖKMEN

Tez Danışmanı
Prof. Dr. İlhami YAVUZ

İstanbul, 2007

ÖZET

Elektronik seçim sistemleri, kâğıt oy pusulası ile oy kullanımını elektronik araçlar ile gerçekleştirmeyi amaçlar. Bu amacın çıkış noktası; seçimin etkin ve güvenilir bir şekilde yapılmasını sağlamak ve insan faktörünün meydana getirebileceği hata ve sahtekârlıkların önüne geçmektir.

Kullanım şekillerine göre farklı elektronik seçim türleri mevcuttur. Bu çalışma; Internet gibi açık ve güvensiz kanallar üzerinde elektronik seçim protokollerinin nasıl çalıştığını incelemekte, farklı oy kullanım modelleri üzerinde durmaktadır. Bu modellerin geniş çaplı bir seçim sistemi için uygulanabilir olup olmadıkları ve daha önceki kullanım şekilleri anlatılmaktadır. Bu modellerden biri olan kriptolojik homomorfizm ile etkin ve güvenilir bir seçim sisteminin nasıl tasarlanabileceği ve önceki çalışmaların neler olduğu incelenmektedir.

Çalışmanın sonunda; Pailler sisteminin homomorfik özelliği üzerine kurulu yeni bir seçim sistemi önerilmektedir.

Anahtar Kelimeler: Elektronik oy**,** elektronik seçim protokolleri, açık anahtar kriptolojisi, kriptolojik homomorfizm, sıfır bilgi ile ispat, Paillier kripto sistemi.

ABSTRACT

Electronic voting systems aim to change paper voting procedures with electronic ones. Main reason for developing such systems is to build a secure and efficient voting system while avoiding human defects.

Election systems vary due to their voting procedures. In this paper; different kinds of voting models is examined. It is also studied how voting protocols run on unsecure channels and these are analysed whether they can be used to build an efficient and secure voting system.

At the end of this thesis; a new voting system based on Paillier homomorphism is proposed.

Keywords: Electronic voting**,** voting protocols, public key cryptology, homomorphic encryption, zero knowledge proof, Paillier cryptosystem.

TEŞEKKÜR

Bu çalışmada emeği geçen Prof. Dr. İlhami Yavuz Hocama ve değerli yorumları için Öğ. Gör. Şenol Zafer Erdoğan 'a teşekkür ederim.

İÇİNDEKİLER

KISALTMALAR LİSTESİ

PIN	Personal Information Number (Kişisel bilgi numarası)
BB	Bullettin Board (Mesaj panosu)
DoS	Denial-of-Service (Kaynaklarının servis veremez duruma gelmesi)
MIX	Karıştırmak
ZKP	Zero Knowledge Proof (Sıfır bilgi ile ispat yöntemi)
RSA	Rivest, Shamir, Adleman (Açık anahtar şifreleme teknolojisi)
SSL	Secure Socket Layer (Güveli haberleşme katmanı)
TLS	Trasport Layer Security (İletişim katmanı güvenliği),
SSH	Secure Shell (Güvenli kabuk)
EKE	Encrypted Key Exchange (Şifreli anahtar değişimi)
SRP	Secure Remote Password (Güvenli şifreli erişim)

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

1. GİRİŞ

Elektronik seçim sistemleri, kriptolojinin en ileri çalışma alanlarında biridir. Kâğıt oy pusulaları ile oy kullanımını, elektronik aletler ile etkin ve güvenli bir şekilde gerçekleştirmeyi hedefler. Bununla beraber, kişilere bağlı hata ve sahtekârlıkların önüne geçmek ve demokrasi sürecini iyileştirmek bu sistemlerin yaygınlaşması ile mümkün olabilir.

Elektronik seçim sistemleri, oy kullanımına göre farklılıklar gösterir. Geniş ölçekli seçimlerde (genel seçim ve referandumlar gibi) elektronik oylar seçim merkezlerinde kullanılır. Seçim merkezleri ile oyların toplandığı merkezi otoriteler arasında güvenli bir iletişim ağı mevcuttur. Oy makineleri seçim için özel geliştirilmiş yazılım ve donanımlara sahiptirler. Böylece toplumun her kesiminden kişilerin – sağır, dilsiz veya sakat dahi olsa – seçim sürecine katılmaları beklenir. Oy kullanımı farklı bir şekilde internet gibi herkese açık fakat güvensiz kanallar üzerinde yapılabilir. Kriptolojik protokoller ile desteklenecek böyle bir seçimde oy kullanıcıları, kullandıkları oyları açık kanal üzerinden seçim otoritelerine iletirler. Bu çalışmada; elektronik seçimin açık kanallar üzerinde nasıl gerçekleştirilebileceği incelenmektedir. Diğer seçim türü çalışmanın konusu dışında bırakılmıştır.

Demokratik seçim sistemlerinde kullanıcı ile oy arasında bir ilişki kurulamaz. Oylar kullanıldıktan sonra anonim hale gelirler, kullanıcıları bilinemez. Bu prensip esas alındığında mevcut sistemler üç farklı oylama modeli oluşturur. İlki David Chaum [1] tarafından geliştirilmiş olan MIX-Net modelidir. Kullanıcısı belli olan bir oy, MIX-Net ağı içinde anonim hale gelir. İkinci model, yine David Chaum tarafından geliştirilmiş, kör imza (*blind signatue*) yöntemi ile oy kullanımıdır. Chaum bu yöntemi ilk defa elektronik para uygulamasında kullanmıştır [2]. Bu modelde seçim otoritesi elektronik oyu dijital olarak imzalar fakat oyun içeriği hakkında bilgi sahibi olamaz. Üçüncü model, kripto sistemlerin homomorfik

(yapısal olarak bezer işleve sahip) özellikleri ile anonim oyların üretilmesidir ve bu çalışmada bu model üzerinde durulmaktadır. Diğer iki modelden farklı olarak bu modelde oyların içerikleri açılmaksızın seçim sonucu belirlenebilir.

Internet tabanlı seçim sistemlerinin dünyadaki önemli örnekleri şunlardır:

- İsviçre'de 2003 yılında Cenevre yakınlarındaki bazı bölgelerde halkın yerel referandumlara elektronik olarak katılımı gerçekleştirilmiştir. Bu referandumlar başarılı olunca diğer senelerde daha yüksek katılımlı elektronik referandumlar gerçekleşmiştir [3].
- Estonya 2005 yılı yerel seçimlerini Internet tabanlı elektronik seçim sistemleri ile gerçekleştirmiştir.
- İngiltere2006 yılından sonra elektronik oylamayı hayata geçirmeyi düşünen ülkeler arasındadır. Diğer yandan Avrupa komisyonu tarafından hayata geçirilen Cybervote projesi [4] yüksek güvenlikli internet tabanlı seçim sistemlerini geliştirmektir.

Bu çalışmada; yüksek güvenirlikli, sürecin herkes tarafından izlenebildiği (açık) ve etkin bir elektronik seçim siteminin nasıl kurulabileceği incelenmektedir. Bu konuda yapılmış birçok çalışma elektronik oyun kullanımı üzerine yoğunlaşmış, seçimin diğer süreçleri (kimlik doğrulama, seçim anahtarının dağıtık üretimi, vs.) ayrıntılı incelenmemiştir. Bu yüzden bu çalışmanın diğer çalışmalardan önemli bir farkı; seçim sürecini bir bütün olarak ele alıp incelemesidir. Sürecin matematiksel bir modeli olduğu gibi, bu modelin günümüz bilgi ve haberleşme altyapısı üzerinde gerçekleştirilebilir olmasına özen gösterilmiş ve kriptolojik protokoller bu doğrultuda seçilmiştir.

Bu çalışma şu şekilde bölümlenmiştir: İkinci bölümde; elektronik seçim kavramları üzerinde durulmakta ve farklı yaklaşımlar incelenmektedir. Üçüncü bölümde; kurulacak seçim modelinin kriptolojik alt yapısına değinilmektedir. Dördüncü bölümde, matematik modeli incelenmiş protokoller ile elektronik bir

seçim sisteminin nasıl kurulabileceği gösterilmekte ve Paillier kripto sisteminin homomorfik özelliğinden faydalanan yeni bir yöntem önerilmektedir.

2. MEVCUT SEÇİM MODELLERİ VE YAKLAŞIMLAR

Elektronik seçim sistemi, seçim otoriteleri ve oy kullanıcıları arasında çalışan bir protokoller bütünüdür. Taraflar arasındaki haberleşme, Okamoto [5]' nun önerdiği anonim kanallar üzerinden yapılabileceği gibi herkese açık fakat güvensiz kanallar (Internet ağı) üzerinden de yapılabilir. Anonim kanallar, oy kullanıcısının kimliğini haberleşeme boyunca gizler. Bu kanallarda her bit ayrı olarak şifrelenerek iletilir. Çok yüksek bir bant genişliğine ihtiyaç duyduğundan pratikte uygulanabilir değillerdir. Anonim kanalların bu dezavantajı dikkate alındığında Internet ağının kullanılması kaçınılmazdır.

Açık anahtar kriptolojisindeki gelişmeler bilginin Internet üzerinden güvenli bir şekilde aktarımına olanak sağlar. Demokratik seçimlerde kullanılan oylar anonimdir ve seçim sürecinde oy ile kullanıcısı arasında bir ilişki kurulamaz. Bu yüzden, seçim protokolleri için yapılan çalışmalar daha çok oy kullanımı üzerine yoğunlaşmıştır.

2.1. Güvenilir ve Doğrulanabilir Elektronik Seçim Sisteminin Özellikleri

Seçim modelinin kurulmasında, modelin bağlı kalacağı tanımlamaların yapılması gereklidir. Seçim sisteminin ne kadar etkin, güvenilir ve doğrulanabilir olduğu bu sayede ölçülebilir.

- *Yetki:* Sadece oy kullanmaya yetkili kullanıcılar oy kullanabilirler.
- *Gizlilik:* Seçimi gözlemleyen biri, oy ile kullanıcısı arasında ilişki kuramaz.

- *Kullanıcı tarafından doğrulama:* Her kullanıcı oyunun sayıldığından emin olmalıdır.
- *Herkes tarafından doğrulama:* Seçimi dışarıdan izleyen bir gözlemci seçimin adil olduğunu ve seçim sonucunun tüm geçerli oyların sayılması ile hesapladığını doğrulayabilmelidir.
- *Doğruluk***:** Katılımcılar oyların sayımından önce seçim sonucu hakkında kısmi bilgiye sahip olamazlar. Bu sonuç henüz oy kullanmamış kişilerin fikirlerini etkileyebilir.
- *Sağlamlık***:** Seçim sürecini bozmak veya aksatmak için yapılacak girişimler seçim sürecini etkilememelidir. Böyle bir girişim sistem tarafından fark edilebilir olmalıdır.
- *Reçetesiz oy kullanımı***:** Kullanılan oyun yazılı bir kopyası kullanıcıya verilmemelidir. Bu sayede oy satın alma veya belli yönde oy kullanımı için zorlamalar önlenebilir.

2.2. Elektronik Seçim Modelini Oluşturan Unsurları

*Oy Kullanıcıları***:** Elektronik oy kullanımı, kullanıcıların en az çaba ve zaman ile yapabilecekleri şekilde tasarlanmalıdır. Seçim sürecinde oy kullanmaya yetkili kişiler, yetkili olduklarını gösteren özel şifre veya sertifikalarla sisteme giriş yaparlar ve istedikleri aday/düşünce için oylarını kullanırlar. Kullanılan oylar şifrelenen haberleşme kanalları ile seçim otoritelerine iletilir.

*Seçim Otoriteleri***:** Seçim otoriteleri seçimi yönetirler. Oyların toplanması, sayılması ve sonuçların açıklanması için farklı otorite grupları kullanılabilir. Normal bir seçim sürecinde , $t \leq N$ olmak üzere, N otoriteden t tanesinin seçimin temel prensiplerini ihlal edecek (DoS saldırıları, oy değiştirme, kullanıcıların kimliklerini

elde etme) girişimlerde bulunabileceği varsayılır ve *t* güvenlik parametresi seçimden önce belirlenmelidir (Eşik değerli paylaşım). Eğer *t+1* hilekâr otorite işbirliği yaparak seçime hile karıştırırsa seçim amacına ulaşamaz.

*Aktif Saldırılar***:** Seçim sürecini bozmak veya aksatmak için otoriteler, oy kullanıcıları veya üçüncü grup kişiler tarafından yapılır. DoS saldırıları, kullanıcı gizliliğini ihlal edecek saldırılar, seçim veritabanını okumak veya değiştirmek için yapılacak girişimler, otoritelerin bilerek yetkisiz kişilerin sisteme girişine veya seçmenlerin birden fazla oy kullanmasına izin vermesi, kullanılmış oyların yok edilmesi aktif saldırılara örnek olarak verilebilir.

Mesaj Panosu (Bulletin Board - BB): Belli bir görüş ve düşünceyi paylaşmak için bir araya gelen insanların oluşturdukları haberleşme ortamıdır. Internetin yaygınlaşması ile önemleri artmıştır. Benaloh [6] ilk defa elektronik seçimlerde mesaj panolarından nasıl yararlanıldığını göstermiş, bu şekilde tasarlanan bir seçimin herkes tarafından doğrulanabilir olduğunu belirtmiştir. Doğrulanabilir seçim sistemlerinde bu yaklaşımın yaygın olarak kullanıldığı görülmektedir. Mesaj panoları yazılım olarak gerçeklenirler (Seçim otoritelerinin web sayfaları, vs.). Kullanıcılar sadece kendilerine ait alanlara yazabilirler. Gönderilen oylar yalnızca seçimin gizli anahtarı ile şifrelenir. Mesaj panosuna gönderilen oyların geçerlilikleri ispatlanabilir fakat oyların içerikleri hakkında bilgi sahibi olunamaz.

2.3. Oylama Türleri

Seçim modeli tasarlanırken oylamanın türü önceden belirlenmelidir. Oyların sayımı için oyların nasıl bir şekilde kodlandığı bilinmelidir. Hatalı kodlanmış oylar seçim otoriteleri tarafından geçersiz sayılır. Oylamanın karmaşıklığı, seçim modelinin tasarımını zorlaştıran bir unsurdur.

*Evet/Hayır oylama***:** Oyun evet ya da hayır olabileceği oylama şeklidir. Referandumlar bu oylamaya örnek verilebilir. Tasarımı en kolay oylama şeklidir. 1/0 veya 1/-1 olarak ifade edilen oyların toplamı seçimin sonucunu belirler. Seçimin güvenirliğini arttırmak için oy kullanıcısı, toplamları oyun sayısal değerine eşit ve sayıları otorite sayısı kadar olan rasgele sayılar seçer ve bunları otoriteler arasında paylaştırır (Tablo 2–1).

Tablo 2-1 Oyun otoriteler arasında paylaştırılması

Oy	*Otorite 1*	*Otorite 2*
Evet	1001	-1000
Hayır	750	-751
Evet	501	-500
Toplam	2252	-2251
Sonuç	1 (Evet)	

Her otorite kendine ait parçaları toplar ve mesaj panosunda yayınlar. Bu parçaların toplamı seçim sonucunu belirler.

N adaydan birinin oylanması: Parti başkanları, başbakan veya cumhurbaşkanı seçimi bu oylama türüne örnek verilebilir. Oylar *1...N* arasındaki sayılar şeklinde veya her aday için evet/hayır oyu kullanılarak kodlanabilir.

N adaydan k tanesinin oylanması: En genel oylama türüdür. Oylar her aday için evet veya hayır şeklinde kodlanabilir.

Yazılabilir oylar: Kiayias ve Yung [7] geliştirdikleri seçim modeli ile oyun kodlanmasını veya açık olarak yazılmasını kullanıcıya bırakmıştır.

2.4. Oy Kullanımı İçin Temel Modeller

Temel oylama modelleri, oy ile kullanıcı arasındaki ilişkiyi ortadan kaldırarak oy kullanımını anonim hale getirmek için üç ana grup altında toplanmıştır.

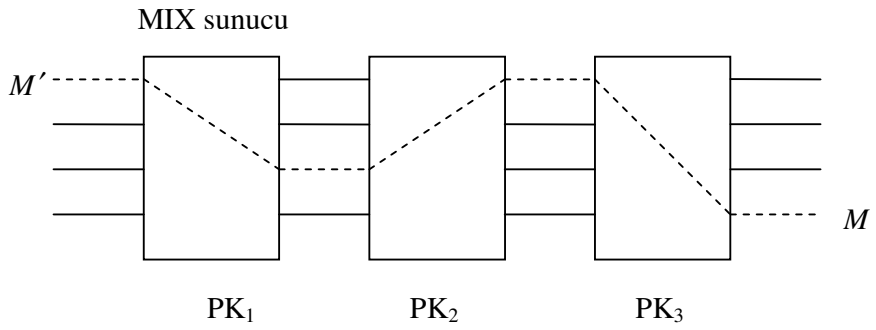
2.4.1. MIX-Net ağ modeli

Ana fikri 'karıştır ve şifrele' olan bu yaklaşım ilk olarak David Chaum tarafından 1981 yılında anonim elektronik posta göndermek amacıyla geliştirilmiştir [1]. Sonraki yıllarda elektronik seçim sistemlerinde bu model benimsenmiştir ([8], [9], [10], [11], [12], [13]). Bu ağların işlevi gönderilen bilginin anonim olmasını sağlamak, gönderici ile gönderilen bilginin ilişkisini ortadan kaldırmaktır. Göndericinin kimliği ağın ilk elemanı tarafından, gönderilen bilginin içeriği ise eğer başka bir gizli anahtar ile şifrelenmemişse, ağın son elemanı tarafından bilinebilir. Bu ağlar MIX adı verilen sunucu bilgisayarlardan oluşur.

MIX ağlarının farklı kullanım şekilleri mümkündür. İlk kullanım şeklinde sunucular kendilerine gelen oyları rasgele bir sırada karıştırır ve bir sonraki sunucuya aktarırlar. Bilginin ağ içerisinde izlenememesi için rota seçimi rasgele yapılır. Sunucular kendilerine gelen bilgileri gizli anahtarları ile çözer, bir sonraki sunucunun açık anahtarı ile şifrelerler [1].

David Chaum 'un çalışmasında ise bilginin izleyeceği rota bellidir. Anonim hale getirilecek bilgi rota üzerindeki her sunucunun açık anahtarı ile iç içe şifrelenir. Her katmandaki sunucu, gizli anahtarı ile bilgiyi bir kat açar ve diğer sunucuya

gönderir Şekil 2.1' de rota üzerindeki son sunucu bilgiyi kendi gizli anahtarı ile çözdüğünde kullanıcının iletmiş olduğu asıl bilgi elde edilir.



Şekil 2.1 David Chaum 'un öngördüğü MIX-Net modeli

Şekil 2.1 'de Chaum tarafından geliştirilmiş MIX Net modeli görülmektedir. *PK* açık anahtar şifreleme fonksiyonu ve *M* gönderilecek mesaj içeriği olmak üzere M' ve M arasındaki ilişki denklem 2.1 'de gösterilmiştir.

$$M' = PK_1(PK_2(PK_3(M))) \tag{2.1}$$

MIX Net için bilinen en ciddi saldırı bir sunucunun diğer sunucuya yanlış bir bilgi göndermesi durumudur (*substition attack*). Bu saldırıları önlemek için her sunucu, giriş ve çıkış değerlerinin aynı bilgiye ait olduğunu sıfır bilgi ile ispat (ZKP) yöntemini kullanarak ispatlar [14]. Chaum' un öngördüğü modelde işlev dışı kalan bir sunucu ağın devre dışı kalmasına sebep olmaktadır.

2.4.2. Kör imza modeli

Elektronik imzalar, açık anahtar sistemlerinde kullanılan anahtar çiftleri (açık ve gizli anahtar) ile üretilir ve doğrulanırlar. İmzası üretilecek bilgi çok büyük

olabileceğinden, bilginin kendisi yerine bir özet fonksiyonu (*hash function*) yardımıyla üretilen sayısal özeti imzalanır. Özet fonksiyonları değişken boyutlu bir bilgiyi sabit uzunlukta sayısal bir değere dönüştüren tek yönlü fonksiyonlardır. Özet bilgiden asıl metni elde etmek pratikte uygulanabilir değildir. Bilgiyi imzalayacak kişi kendi gizli anahtarı ile özet bilgiyi şifreler ve asıl metne ekler. Metnin üzerindeki imza herkes tarafından doğrulanabilir.

Gizlilik esaslı bir protokol olan kör imza yöntemi elektronik imzanın farklı bir kullanımıdır. İlk defa David Chaum [2] tarafından elektronik para uygulamasında kullanılmıştır. Bundan sonra diğer elektronik para uygulamalarının temel modelini oluşturmuştur ([15], [16], [17], [18], [19]).

Bu yöntemin elektronik imzadan temel farkı bilginin imzalayan tarafından bilinememesidir. Asıl bilgi rasgele seçilmiş bir sayı ile maskelenir ve yeni değer imzalanır. Maskeleme bilgisi ortadan kaldırılarak asıl bilginin imzası elde edilir.

Kör imza modeline elektronik seçimlerde sıklıkla başvurulmuştur ([20], [21], [22], [23], [24]). Bu modelde, yalnızca otoriteler tarafından imzalanmış oylar geçerlidir. Kullanıcı, oyunu imza otoritesine kör imza yöntemiyle imzalatır. Otorite imzalama sırasında oyun içeriği hakkında bilgi sahibi değildir, sadece maskelenmiş yeni değeri bilebilir. Kullanıcı son olarak oyu ve gizli seçim anahtarı ile imzalanmış dijital imza bilgisini sayım otoritesine gönderir.

David Chaum kör imza yöntemini RSA imzalama yöntemini kullanarak geliştirmiştir. Bunun yanında ayrık logaritma problemi çözümünün zorluğuna dayanan kör imza yöntemleri de mevcuttur ([25]). RSA imzası m bilgisinin sadece imzalanan tarafından bilinen gizli bir d üssünün herkese açık bir n sayısına göre modülü alınarak hesaplanır.

$$s \equiv m^d \bmod n \;\; s \tag{2.2}$$

Kör imza yönteminde imzalanacak bilgi *r* gibi rasgele bir sayı kullanılarak imzalayan kişiden gizlenir. *e* değeri RSA kripto sisteminin açık değeri olup *d* gizli değerinin n modülüne göre tersidir.

$$\gcd(r, n) = 1 \tag{2.3}$$

$$ed \bmod n = 1 \tag{2.4}$$

Denklem 2.3 ve denklem 2.4 eşitlikleri sağlanmak koşulu ile r^e gizleme faktörü olarak kullanılır. Kullanıcı açık *m* mesajı yerine, $m(r^e)$ ifadesini otoriteye imzalatır. Böylece otorite m değeri hakkında bilgi sahibi değildir.

$$s' \equiv (m(r^e))^d \bmod n \tag{2.5}$$

$$s' = m^d r \bmod n \tag{2.6}$$

Denklem 2.7' de gizleme faktörünün tersi alınarak asıl imza bilgisinin nasıl üretildiği gösterilmektedir.

$$s \equiv (s' * r^{-1}) \bmod n \equiv m^d r * r^{-1} \bmod n = m^d \bmod n \tag{2.7}$$

2.4.3. Homomorfik şifreleme modeli

E, açık anahtar şifreleme fonksiyonu ve $E(x_1)$, $E(x_2)$ ise iki şifreleme ifadesi olmak üzere, x_1 ve x_2 değerleri kullanılarak yapılacak cebirsel bir işlem $E(x_1)$ ve $E(x_2)$ ifadelerini de kullanarak gerçekleşebiliyorsa *E* 'nin homomorfik bir şifreleme fonksiyonu olduğu söylenir [26]. "*" homomorfik bir işlem olmak üzere bu özellik denklem 2.8' de gösterilmektedir.

$$E(x_1) * E(x_2) = E(x_1 * x_2) \tag{2.8}$$

Farklı kripto sistemler farklı homomorfik özelliklere sahiptirler. El-gamal ve RSA kripto sistemleri çarpımsal homomorfik iken, Paillier ve Benaloh kripto-sistemleri toplamsal homomorfiktirler. Çarpımsal homomorfik sistemlerde iki ifadenin çarpımının şifrelenmesi, ifadelerin şifreli hallerinin çarpımına eşittir. Toplamsal homomorfik sistemlerde ise ifadelerin toplamının şifreli hali, şifreli hallerinin çarpımına eşittir.

Paillier Homomorfizmi: Paillier kripto sistemi $Z_{n^2}^*$ üzerinde çalışan olasılıksal (*probabilistic*) bir kripto sistemdir ve şifreleme ifadesi toplamsal homomorfiktir. Bir m mesajının şifrelenmesi, g grup üreteci ve $r \in Z_{n^2}^*$ 'den seçilmek üzere denklem 2.9 'da gösterilmektedir.

$$E(x) = g^x r^m \bmod n \tag{2.9}$$

Bu kripto sistemin toplamsal homomorfizmi denklem 2.10 ile gösterilmektedir.

$$E(x_1) \,.\, E(x_2) = (g^{x_1} r_1^m)(g^{x_2} r_2^m) = g^{x_1 + x_2} (r_1 r_2)^m = E(x_1 + x_2 \bmod n) \tag{2.10}$$

1 (evet) ve 0 (hayır) oylarından oluşan basit bir seçim sisteminde şifreli oyların çarpımı evet oylarının şifrelenmiş bir toplamı olacağından oyların içerikleri açılmadan seçim sonucu belirlenebilir. Kullanıcı ve oy gizliliğini önemli derecede sağladığı için homomorfik sistemler elektronik seçim sistemlerinde yaygın olarak tercih edilirler ([27], [6], [28], [12], [29], [30], [31], [32], [33], [34]).

3. KRİPOLOJİK ALTYAPI

Elektronik seçim sistemleri tasarlanırken farklı kripto sistemler ve farklı sayı grupları üzerinde çalışan kriptolojik protokol ve yöntemlerden faydalanılır. Bu bakımdan elektronik seçim sistemleri kriptolojinin en ileri çalışma konularından biridir.

Sıfır bilgi ile ispat yöntemlerinin yaygınlaşması, oy bilgisinin gizliliğini esas alan seçim sistemlerinin daha kolay tasarlanmasını mümkün kılmıştır. Böyle tasarlanmış bir sistemde kullanıcılar oylarını seçim otoritesi dâhil olmak üzere hiç kimseye göstermeden kullanabilirler. Bu çalışma büyük ölçüde sıfır bilgi ile ispat yöntemlerini incelemektedir.

Kullanıcıların birden fazla oy kullanmasını önlemek ve oy kullanmaya yetkili olup olmadıklarını sınamak için kimlik doğrulama (*authentication*) protokollerinden yararlanılır. Doğrulama basit bir şifre denetimi şeklinde olabileceği gibi, tarafların açık anahtarlarının bulunduğu sertifikaların değişimi şeklinde de yapılabilir.

Haberleşen taraflar arasındaki iletişimin güvenliği haberleşme kanalının şifrelenmesiyle mümkündür. Şifreleme simetrik veya asimetrik olabilir. İnternet haberleşmesi için en güvenilir çözüm SSL veya TLS gibi karma protokol yığınlarının kullanılmasıdır. Bu protokol yığınları, dijital sertifikalar yardımıyla simetrik şifreleme, asimetrik şifreleme ve anahtar değişimi gibi protokolleri en etkin bir şekilde kullanarak haberleşme kanalının güvenliğini sağlarlar.

Seçim sistemlerinde oyun kullanılması için farklı yaklaşım modelleri (homomorfik şifreleme, MIX Net ağları ve kör imzalar) öngörülmüştür. Geçerli oyların sayılması oyların kullanım şekline göre değişmektedir. Homomorfik oylama sistemlerinde seçim sonucunu belirlemek için oyların açılmasına gerek duyulmaz.

MIX Net ağları ile kullanılan oylar anonim hale getirildikten sonra açılarak sayılır. Kör imza tabanlı oylama sistemlerinde ise gizlilik yeterli derecede sağlanamaz. Çünkü hangi kullanıcının hangi şifreli oyu kullandığı bilgisi hilekâr otoriteler tarafından not edilebilir. Bu yüzden bu sistemler tek başına uygulanabilir değillerdir. Oyun anonim olarak iletilmesi bu açıdan çok önemlidir.

Oyların sayımı sürecinde, şifreli oyları çözecek birden fazla otoritenin varlığı ve seçimin gizli anahtarının bu otoriteler arasında paylaştırılması seçimin güvenirliğini attıracaktır.

3.1. Eşik Değerli Gizli Paylaşım (Secret Sharing) Protokolü

Çok otoriteli bir seçim sisteminde *s* gizli seçim anahtarının *N* otorite arasında paylaştırılmasına ve $t \leq N$ olmak üzere en az *t+1* otoritenin bir araya gelerek *s* değerini geri oluşturmasına eşik değerli gizli paylaşım protokolü denir. *t* ve daha az sayıda otorite koalisyonu *s* bilgisini geri getiremez. *t* bir sistem parametresi olup hilekar otorite sayısını belirler. Hilekâr otorite sayısı bu değerden büyük ise seçimin demokratik olamayacağı söylenebilir. *(t+1,N)* gizli paylaşım protokolü olarak da bilinen bu yöntem Adi Shamir tarafından geliştirilmiştir ([35]). Bu protokole göre gizli bir değerin paylaştırılması ve geri oluşturulması aşağıdaki adımları içerir.

1. Derecesi *t*, sabit terimi *s* olan ve diğer katsayıları rasgele seçilmiş bir *f(x)* polinomu seçilir (Denklem 3.1, denklem 3.2). Polinom seçimi tüm katılımcılar tarafından bilinen sonlu bir *F* cismi (*field*) üzerinde yapılır.

$$s = \alpha_0, s \in F \tag{3.1}$$

$$f(x) = \alpha_0 + \alpha_1 x + ... + \alpha_t x^t \quad , \; f(0) = s \tag{3.2}$$

2. Her A_j otoritesi için $s_j = f(j)$ gizli değer parçası üretilir.
3. $t+1$ otoritenin gizli parçalarından oluşacak bir A kümesi lagrange enterpolasyon yöntemi ile s değerini geri oluşturabilir (Denklem 3.3, denklem 3.5).

$$s = f(0) = \sum_{j \in A} f(j)\lambda_{j,A} = \sum_{j \in A} s_j \lambda_{j,A} \tag{3.3}$$

$$\lambda_{j,A} = \prod_{l \in A - \{j\}} \frac{l}{l-1} \tag{3.4}$$

Bu protokolde parçaların oluşturması güvenilir bir hakem tarafından yapılır. Birleştirme sırasında protokole katılan otoritelerin doğru parçaları gösterdikleri bu protokol ile tek başına ispatlanamaz. Adi Shamir' in geliştirdiği bu yöntem üzerine Schoenmaker [36] doğrulanabilir bir gizli paylaşım protokolü geliştirilmiştir.

3.2. Paillier Kripto Sistemi

Pascal Paillier, n. dereceden kalan sınıflarının (*composite residuosity class*) hesaplanmasının zorluğuna dayanan ve $Z^*_{n^2}$ grubu üzerinde çalışan olasılıksal asimetrik bir kripto sistem geliştirmiştir ([26]).

Komposit kalan sınıfı: $z \equiv y^n \bmod n^2$ iken $y \in Z^*_{n^2}$ gibi bir sayı var ise z sayısının n^2 modulüne göre n. dereceden bir kalan olduğu söylenir. n. dereceden kalanların oluşturduğu küme $Z^*_{n^2}$'in çarpımsal bir alt kümesidir.

Komposit kalan sınıflarını polinomial zamanda çözecek bir yöntem mevcut değildir. Bu yüzden Paillier kripto sistemi semantik olarak güvenli kabul edilir. Aynı zamanda toplamsal homomorfik bir kripto sistemdir. Çarpımsal homomorfik olan bazı kripto sistemler farklı gösterimler ile toplamsal homomorfik hale gelebilirler. Denklem 3.6 El-Gamal kripto sisteminin (denklem 3.5) nasıl toplamsal homomorfik hale gelebildiğini gösterir (g grup üreteci, m şifrelenecek mesaj, c şifreli metin).

$$E(m) = (g^k \bmod p, my^k \bmod p) \tag{3.5}$$

$$E_T(m) = (g^k \bmod p, g^m y^k \bmod p) \tag{3.6}$$

Denklem 3.6 'da, g^m ifadesinde ki m değerini tek seferde elde etmenin basit bir yolu yoktur ve ayrık logaritma probleminin çözümünü gerektirir. Bu yüzden toplamsal homomorfik tasarlanacak bir sistemde Paillier kullanımı daha etkin sonuçlar verecektir.

Paillier kripto sisteminin diğer önemli bir özelliği şifrelenen aynı sayıların farklı sonuçlar üretmesidir (*self blinding*). Bu özelliğin seçim sistemlerindeki en önemli avantajı aynı seçim anahtarı ile şifrelenmiş aynı oyların farklı sayılarla ifade edilebilir olmasıdır.

Anahtar üretimi: p ve q asal sayılar, $n = pq$ ve $g \in Z^*_{n^2}$ olmak üzere denklem 3.6, denklem 3.7 ve denklem 3.8 eşitliklerini sağlayan rasgele bir g seçilir.

$$\lambda = lcm((p-1)(q-1)) \tag{3.7}$$

$$L(u) = \frac{u-1}{u} \tag{3.8}$$

$$\gcd(L(g^\lambda \bmod n^2), n) = 1 \tag{3.9}$$

Açık anahtar (n, g) ve gizli anahtar λ olarak belirlenir.

Şifreleme: $m \in Z_n$ mesajını şifrelemek için rasgele bir $r \in Z^* n$ seçilir ve denklem 3.10' deki şekliyle *m* mesajı şifrelenir.

$$c = g^m r^n \bmod n^2 \tag{3.10}$$

*Şifrenin çözülmesi***:** c şifreli mesajı denklem 3.11 yardımıyla çözülür. *L* fonksiyonu parametre olarak denklem 3.12' deki S_n kümesi elemanlarını kabul eder.

$$m = L(c^\lambda \bmod n^2)/(L(g^\lambda \bmod n^2)) \tag{3.11}$$

$$S_n = \{u < n^2 \mid u = 1 \bmod n\} \tag{3.12}$$

3.3. Dağıtık Anahtar Üretimi ve Eşik Değerli Deşifre (Threshold Decryption)

Otoritelerin, oyların içeriklerini öğrenmesini engellemek ve kullanıcı gizliliğini korumak için oyları çözecek gizli anahtarın otoriteler arasında paylaştırılması gerekir. t, seçimden önce belirlenen bir güvenlik parametresi olmak üzere paylaşım *N* otorite arasında yapılır. Bu durumda *t+1* otoritenin bir araya gelmesiyle gizli seçim anahtarı birleştirilir.

Anahtar üretimi ve dağıtımı, güvenilir bir hakemin katılımı ([31], [37], [38]) veya dağıtık bir paylaştırma protokolü ([39], [40]) ile yapılabilir. Eğer anahtar üretimi bir hakem tarafından yapılıyorsa, üretilen parçalar dağıtımdan sonra yok edilmelidir.

Eşik değerli ilk Paillier kripto sistemi Baudron, Fouque ve Stren [31] tarafından geliştirilmiştir. Bu kripto sistem RSA tabanlı dağıtık imzalama yöntemi esas alınarak tasarlanmıştır [37].

Anahtar üretimi ve paylaşımı: *p, q* güçlü asal sayılar (*strong primes*) ve $n = pq$, $\gcd(n, \phi(n) = 1$ olmak üzere denklem 3.13 ve denklem 3.14 eşitliklerini sağlayacak p' ve q' asal sayıları seçilir ve *m* değeri hesaplanır.

$$p = 2p' + 1 \tag{3.13}$$

$$q = 2q' + 1 \tag{3.14}$$

$$m = p'q' \tag{3.15}$$

Rasgele bir $\beta \in Z_n^*$ değeri ve $(a,b) \in Z_n^* x Z_n^*$ ikilisi belirlenir. Bu değerler ikinci dereceden bir kalan sınıfı olmayan g ifadesinin üretilmesi için kullanılır (denklem 3.16).

$$g = (1+n)^a b^n \bmod n^2 \tag{3.16}$$

$\beta.m$ çarpımı gizli anahtar olarak belirlenir ve Shamir gizli anahtar paylaşım yöntemiyle otoriteler arasında paylaştırılır (denklem 3.17, denklem 3.18). Paylaşım sonunda her otorite kendine ait gizli bir s_i parçası elde eder (denklem 3.19).

$$a_0 = \beta.m \tag{3.17}$$

$$f(x) = \sum_{i=0}^{t} a_i x^i \quad , \; a_i \in \{0, \ldots, n \times m - 1\} \tag{3.18}$$

$$s_i = f(i) \bmod n \times m \tag{3.19}$$

Açık anahtar bilgileri *g, n* ve θ (denklem 3.20) olarak yayınlanır.

$$\theta = L(g^{m\beta}) = am\beta \bmod n \tag{3.20}$$

Gizli paylaşımın doğrulanabilir olması için her gizli anahtar parçası için bir doğrulama bilgisi oluşturulmalıdır. Bunun için; $Z_{n^2}^*$ grubunu (*cyclic group*) oluşturacak bir *v* grup üreteci (*group generator*) seçilir. Her otorite anahtarın oluşturulması sırasında anahtarın değiştirilmediğini gösteren bir doğrulama ifadesi üretir (denklem 3.21).

$$v_i = v^{\Delta s_i} \bmod n^2, \quad \Delta = n! \tag{3.21}$$

Şifreleme: *m* mesajını şifrelemek için rasgele bir $r \in Z_n^*$ seçilir ve Paillier kripto sistemin şifreleme ifadesi (denklem 3.10) kullanılarak şifreli c mesajı üretilir.

Şifreli mesajın parçalı çözümü: Her otorite $c_i = c^{2\Delta S_i}$ değerini hesaplar ve kendine ait gizli anahtar parçasının (s_i) doğruluğunu ispatlar (denklem 3.22).

$$\log_v(v_i) \bmod m \times n = \log_{c^4}(c_i^2) \bmod m \times n \tag{3.22}$$

Parçaların birleştirilmesi: Doğruluğu ispatlanan parça sayısı seçimin güvenlik parametresi *t* 'den az ise birleştirme işlemi başarısızdır. Eğer yeterli sayıda (*t+1* veya daha fazla) otorite koalisyonu sağlanırsa anahtar üretimi başarılı demektir.

S kümesi, en az *t+1* geçerli gizli parçanın oluşturduğu bir küme olduğu düşünülürse denklem 3.23 ve denklem 3.24 yardımıyla *m* mesajı geri üretilir.

$$\mu_{0,j}^S = \Delta \times \prod_{j' \in S-\{j\}} \frac{j'}{j'-j} \in Z \tag{3.23}$$

$$m = L(\prod_{j \in S} c_j^{2\mu_{0,j}^S} \bmod n^2) \tag{3.24}$$

3.4. Sıfır Bilgi İle İspat (*Zero Knowledge Proof - ZKP*)

Sıfır bilgi ile ispat yöntemi (ZKP) kriptolojik bir ispat yöntemidir. Şifreli bir ifade için yapılan bir iddia ifadenin içeriğini göstermeksizin ZKP yöntemleri ile ispatlanabilir. Bu ispat deterministik bir ispat yöntemi değildir. İddianın doğruluğu olasılıksal (*probabilistic, non-deterministic*) bir ispat olup çok küçük bir olasılıkla bile doğrulayan tarafın kandırılma ihtimali vardır [41]. ZKP yöntemleri aşağıdaki üç özelliği sağlamalıdırlar:

1. *Bütünlük***:** Eğer iddia doğru ise, adil bir ispatlayıcı adil bir doğrulayıcıyı ikna edebilir.
2. *Sağlamlık***:** Eğer iddia yanlış ise, adil olmayan bir ispatlayıcı çok küçük bir olasılık dışında adil bir doğrulayan tarafı iddianın doğruluğuna inandıramaz.
3. *Bilginin gizliliği***:** Üzerine iddia edilen bilginin içeriği öğrenilemez.

ZKP yöntemleri bu özellikleri sayesinde elektronik seçim sistemlerinin vazgeçilmez birer unsuru haline gelmiştir. Özellikle kullanıcı gizliliğinin yüksek olduğu seçim sistemlerinde şifrelenmiş oyun içeriği gösterilmeden oy ile ilgili ispatlar gerçekleştirilebilir. Seçim sürecini dışarıdan izleyen bir gözlemci şifrelenmiş oyları görebilir, oyların geçerli olup olmadığını doğrulayabilir.

Bu bölümde elektronik seçim sisteminin tasarımında kullanılacak bazı ispat yöntemleri incelenmektedir. Bu yöntemler Paillier kripto sistemi ile şifrelenmiş elektronik oyların içeriklerinin geçerli olup olmadıklarının ispatında kullanılmaktadır [41].

3.4.1. Bir ifadenin n. dereceden üs olup olmadığının ispatı

Oyların evet veya hayır (1/0) şeklinde kullanıldığı bir seçim sisteminde Paillier kripto sistemi ile şifrelenmiş *m* oyunun 0 olması durumunda şifreleme ifadesi rasgele seçilmiş bir $r \in Z_n^*$ değerinin *n.* dereceden üssüdür (denklem 3.25).

$$c = g^m r^n \bmod n^2 = r^n \bmod n^2, \qquad m = 0 \tag{3.25}$$

Şifreli bir Paillier ifadesinin içeriğinin $u = v^n \bmod n^2$ formunda olup olmadığının ispatı, ispatlayan(*P*) ve doğrulayan(*V*) arasında aşağıdaki protokol ile gerçeklenebilir:

Açık değerler: u ve *n*

P için gizli değer : $\{ v \mid u = v^n \bmod n^2 \}$

1. *P* rasgele bir *r* değeri seçer ve denklem 3.26'daki a değerini V' ye gönderir.

$$a = r^n \bmod n^2 \tag{3.26}$$

2. *V* karşılık olarak *t* bit uzunluğunda rasgele bir *e* değeri seçer ve *P'* ye gönderir.
3. *P,* gelen *e* değeri için denklem 3.27'deki hesaplamayı yapar ve *z* değerini *V'* ye gönderir. V denklem 3.28 'deki eşitliği kontrol ederek iddiayı kabul ya da reddeder.

$$z = rv^e \bmod n^2 \tag{3.27}$$

$$z^n = au^e \bmod n^2 \tag{3.28}$$

Bu ispat yönteminde *n, k* bit uzunluğunda bir sistem modülüdür. $t = k/2$ olmak üzere sahtekar bir *P, V* 'yi $\leq 2^{-t}$ olasılıkla iddiasına inandırabilir [41].

3.4.2. İki ifadeden birinin n. dereceden üs olup olmadığının ispatı

Bölüm 3.4.1 'de anlatılan ispat yöntemi kullanılarak şifreli bir ifadenin iki aday mesajdan biri olup olmadığı ispatlanabilir. *c*, Paillier kripto sistemine göre şifrelenmiş bir mesaj ve i_1, i_2 aday mesajlar olmak üzere *P* ile *V* arasındaki bu protokol aşağıdaki gibi çalışır:

$$u_1 = c / g^{i_1} = (g^{i_1} r^n) / g^{i_1} \bmod n^2 = r^n \bmod n^2 \quad (3.29)$$

$$u_2 = c / g^{i_2} = (g^{i_2} r^n) / g^{i_2} \bmod n^2 = r^n \bmod n^2 \quad (3.30)$$

M, bölüm 3.4.1 'de anlatılan ispat yönteminin bir simülasyonu kabul edilirse, verilen bir *u* ifadesi için *M* simülasyonu çalıştırıldığında ispat sırasında kullanılan *a, e* ve *z* değerleri üretilebilir (denklem 3.26, denklem 3.27).

Açık değerler: n, u_1 ve u_2 (denklem 3.29, denklem 3.30)

P için gizli değer :$\{ v_1 \mid u_1 = v_1^{\,n} \bmod n^2 \}$

1. *P*, n^2 modülüne göre rasgele bir r_1 değeri seçer ve u_2 için *M* simülasyonunu çalıştırarak (işlemi simüle ederek) a_2, e_2, z_2 değerlerini üretir. Ardından a_1 (denklem 3.31) ve a_2 değerlerini *V*' ye gönderir.

$$a_1 = r^n \bmod n^2 \quad (3.31)$$

2. *V* karşılık olarak *t* bit uzunluğunda rasgele bir *s* değeri seçer ve *P* 'ye gönderir.
3. *P*, e_1 (denklem 3.32), z_1 (denklem 3.33) değerlerini hesaplar ve e_1, z_1, e_2, z_2 değerlerini *V* 'ye gönderir.

$$e_1 = s - e_2 \bmod 2^k \quad (3.32)$$

$$z_1 = r_1 v_1^{e_1} \bmod n^2 \tag{3.33}$$

4. *V* son olarak denklem 3.34, denklem 3.35 ve denklem 3.36'daki eşitlikleri kontrol eder. Tüm eşitlikler sağlanıyorsa ispat kabul edilir. Aksi durumda ispat geçersizdir.

$$s = e_1 + e_2 \bmod 2^k \tag{3.34}$$

$$z_1^{\,n} = a_1 u_1^{e_1} \bmod n^2 \tag{3.35}$$

$$z_2^{\,n} = a_2 u_2^{e_2} \bmod n^2 \tag{3.36}$$

3.4.3. Enteraktif ispatların sadeleştirilmesi (Fiat-Shamir Heuristic)

Bölüm 3.4.1 ve bölüm 3.4.2'de anlatılan ispat yöntemleri, doğrulayan ve ispatlayan arasında enteraktif bir şekilde gerçekleşir. İspatlayan tarafın hile yapmaması için iddianın, doğrulayan tarafın belirlediği bir değeri (*challange*) için test edilmesi istenir.

Genel olarak bir ZKP ispatı üç adımda gerçekleştirilir:

1. *P* rasgele bir değer seçer ve ispatlayacağı ifadesinin sonucunu *V* 'ye gönderir.
2. *V* gelen cevaba (*response*) karşılık kendi ürettiği bir değeri *P* 'nin aynı ifadeye göre hesaplamasını ister.
3. *P* kendine gönderilen bu yeni değeri hesaplar ve sınaması için *V*' ye gönderir. *V* gelen değere göre ispatı kabul veya reddeder.

Fiat - Shamir çalışmasında; enteraktif bir ispatın tek bir seferde gerçeklenebilir olduğunu göstermiştir [42]. Bu çalışmaya göre; *H* tek yönlü bir özet fonksiyon olmak

üzere birinci adım sonunda oluşan bir *s* cevabı, *H(s)* şeklinde ikinci adımda *V* 'den gelecek karşılık olarak kullanılabilir. Bu şekilde bir kullanım haberleşmenin getireceği yükü azaltacaktır.

3.5. Kimlik Denetimi ve Doğrulama

Seçim sürecinin demokratik olabilmesi için sadece oy kullanmaya yetkili kişilerin oy kullanabilmesi ve kullanıcının birden fazla oy kullanımının engellemesi gerekir. Bunun ilk adımı seçime katılacak kullanıcıların kimliklerinin doğrulanmasıdır. Kimlik denetimi ve doğrulaması farklı kriptolojik yöntemler ile gerçekleştirilebilir. Burada önemli olan, seçilecek yöntemin elektronik seçim gereksinimlerini tam olarak karşılaması ve seçim için uygulanabilir olmasıdır.

Sertifika tabanlı kimlik denetimi: Dijital sertifikalar, güvenilir sertifika otoriteleri tarafından verilen dijital kimliklerdir ve ait olduğu kişinin açık anahtarını taşırlar. Oy kullanacak katılımcıların sertifikaları, seçim öncesi seçim otoriteleri tarafından saklanır. Seçim sırasında kullanılan oylar kullanıcıların gizli anahtarı ile dijital olarak imzalanır. Seçim otoritesi kendine ulaşan imzayı doğrularsa oyu kabul eder, aksi durumda oy geçersizdir. Dijital sertifikalar açık anahtar altyapısı üzerine kurulu olduklarından kullanımları son derece güvenlidirler. Kullanıcılara ait gizli anahtarların kullanıcı makineleri üzerinde saklanması, çalınma ve kopyalanma riskine karşı, güvenli kabul edilmediğinden yaygın kullanım gizli anahtarların 'smart card' cihazları üzerinde saklamasıdır. Büyük ölçekli seçim sistemleri için sertifika ve elektronik kart maliyetleri çok yüksektir.

Kerberos tabanlı kimlik denetimi: Kerberos, Athena Projesinin bir parçası olarak MIT' de geliştirilen bir kimlik denetim sistemidir [43]. Kerberos, açık bir ağda güvenli bir şekilde kimlik doğrulamasını gerçekleştirmek için tasarlanmıştır.

Sistemin çalışması için güvenilir bir üçüncü hakeme ihtiyaç vardır. Kerberos protokolü, yerel ağ üzerinde belirli bir etki alanında (*domain*) çalışmak için tasarlanmıştır. Internet gibi geniş ağlar için kullanımı mevcut değildir.

Şifre tabanlı kimlik denetimi: Gerçeklenmesi ve kullanımı çok kolay olması sebebiyle en sık başvurulan yöntemlerden biridir. En basit kullanımı; kriptolojik yöntemler ile haberleşme güvenliği sağlanmış bir kanal üzerinden (SSL, SSH veya TLS kanalları) şifre ve kimlik bilgilerinin seçim otoritesine gönderilmesidir. Hattı dinleyen bir kişinin şifreyi elde etmek için saldırması bu şekilde önlenir. Bu sistemlerin en zayıf tarafı, şifrelerin dosya veya veritabanlarında açık olarak saklanmasıdır. Şifrelerin tek yönlü özet bilgilerinin saklanması çözüm olarak görülebilir. Buna göre; kullanıcılar şifrelerinin açık hali yerine özet bilgilerini otoriteye iletir ve otorite bu özetin veritabanında olup olmadığını kontrol eder (*digest authentication*). Bu durumda bile sistemin güvenilir olduğundan kesin emin olunamaz. Çünkü şifrelenmiş veya tek yönlü bir fonksiyon ile gizlenmiş şifreler yaygın olarak kullanılan ve başarılı sonuçlar veren sözlük saldırısı (*dictionary attack*) tehdidi altında olabilir. Kullanıcı şifreleri, kolay hatırlanabilmesi için alfabe karakterlerinden seçilir ve ardı ardına denemelerle kırılmaları ve tahmin edilmeleri mümkündür. Bu yüzden özet olarak saklanmış şifreler tam güvenli kabul edilmezler, sadece şifrelerin ilk bakışta açık olarak görülmesi önlenmiş olur. Şifre tabanlı kimlik denetim sistemlerindeki en ciddi saldırının sözlük saldırısı olduğu düşünülürse bu saldırıya dayanıklı bir yaklaşıma ihtiyaç vardır.

Steven M. Bellovin ve Michael Merritt 'in şifreli anahtar değişimi *(Encrypted key excahnge - EKE*) protokolü ([44], [45]) bu alanda yapılmış önemli çalışmalardandır. Bu protokol ZKP ispat yöntemi üzerine kurulmuştur. Kullanıcı açık şifre yerine EKE şifreleri ile kimliğini doğrulatır. Günümüzde bu yöntemin kaba kuvvet (*brute force*) saldırısına karşı başarısız olduğu ispatlanmıştır.

Şifre tabanlı kimlik denetiminde hiç bir yöntem "güvenli şifreli erişim" (*SRP, secure remote password*) [46] yöntemi kadar başarılı olamamıştır. Bu yöntemde kullanıcı hiçbir zaman açık (*plain*) veya gizlenmiş (*hashed*) bir şifre göndermez, ZKP ispat yöntemleri ile şifreyi bildiğini ispat eder. Bu durumda seçim otoriteleri şifre veya şifreye denk gelebilecek bir bilgi saklamazlar. Bu yöntem sözlük saldırılarına karşı kırılamaz olduğundan, şifre veritabanını ele geçiren bir saldırgan kullanıcıları taklit edemez. Bu yöntemin bilinen tüm şifre saldırılarına karşı dayanıklı olduğu ispatlanmıştır [46].

3.5.1. SRP kimlik denetim protokolü

SRP, Thomas Wu tarafından geliştirilmiş kimlik doğrulama ve gizli anahtar değişim protokolüdür [46]. Bu protokolde kullanıcı kimliği bir şifre yardımıyla doğrulanır. Doğrulama için sunucu sistemde şifreyi doğrulayacak bir bilgi saklanır. Haberleşme kanalının güvensiz olması durumda bile protokolün güvenli çalışacağı söylenebilir. Eğer şifre geçerli ise protokol gizli bir oturum (*session*) anahtarı üretir. Bu anahtar simetrik bir şifreleme anahtarı olarak kullanılır ve haberleşme sırasında hattın güvenilir bir şekilde şifrelenmesini sağlar.

Protokole başlamadan; kullanıcı bir P şifresi ve şifreyi karıştıracak bir s (salt) değeri seçer. H tek yönlü bir özet fonksiyonu olmak üzere denklem 3.37 ve denklem 3.38'deki x ve v değerlerini üretir.

$$x = H(s, P) \tag{3.37}$$

$$v = g^{x} \tag{3.38}$$

Otorite doğrulama bilgisi olarak *v* ve *s* değerlerini saklar. *x,* gerçek şifrenin eşleniği olduğundan otorite tarafından bilinmemelidir; aksi durumda sözlük saldırısına açıktır.

Protokolün anlatımında kullanılacak ifadeler şunlardır:

n, güvenli bir asal sayı (*safe prime*: *q* asal olmak üzere $n=2q+1$) olup tüm işlem sonuçları bu modüle göre hesaplanır.
g, üzerinde çalışılan grubun bir üreteci.
s, şifrenin bulunmasını güçleştirecek rasgele seçilmiş bir sayı (salt).
P, kullanıcı şifresi.
x, kullanıcının *P* ve s değerlerini kullanarak oluşturduğu (denklem 3.37) gizli anahtar.
v, otoritenin şifreyi denetimi için kullandığı doğrulama bilgisi.
u, açık olarak bilinebilen ve haberleşme protokolü için üretilen rasgele bir sayı.
a ve *b,* geçici gizli anahtar çiftleri.
A ve B, geçici açık anahtar çiftleri.
H, tek yönlü bir özet fonksiyonu.
m ve n, iki string ifade.
K, oturum anahtarı.

Yukarıdaki ifadeleri kullanan SRP protokolü aşağıdaki şekilde çalışır:

1. Kullanıcı, otoriteye kimlik bilgisini (kullanıcı adı, kimlik numarası, vs.) gönderir.
2. Otorite, gönderilen kimlik bilgisine karşılık gelen *v*, *s* değerlerini bulur ve *s* değerini kullanıcıya gönderir. Kullanıcı *s* değeri ile *x* gizli anahtarını üretir (denklem 3.37).

3. Kullanıcı $1 < a < n$ koşulunu sağlayan rasgele bir a sayısı seçer. Bu sayı ile geçici olarak kullanacağı açık anahtarı (denklem 3.39) belirler ve otoriteye gönderir.

$$A = g^{a} \tag{3.39}$$

4. Otorite $1 < b < n$ koşulunu sağlayan rasgele bir b sayısı seçer, geçici olarak kullanacağı açık anahtarı (denklem 3.40) belirler ve rasgele bir u değeriyle beraber kullanıcıya gönderir.

$$B = v + g^{a} \tag{3.40}$$

5. Kullanıcı denklem 3.41'deki, otorite ise denklem 3.42'deki S değerini hesaplar. Her iki denklemdeki S değerleri birbirine eşittir.

$$S = (B - g^{x})^{a+ux} \tag{3.41}$$

$$S = (Av^{u})^{b} \tag{3.42}$$

6. Her iki taraf S değerini tek yönlü bir özet fonksiyonundan (H) geçirerek ortak bir oturum anahtarı üretir (denklem 3.43).

$$K = H(S) \tag{3.43}$$

7. Kullanıcı doğru bir oturum anahtarı kullandığını göstermek için M_1 değerini otoriteye gönderir (denklem 3.44).

$$M_1 = H(A, B, K) \tag{3.44}$$

8. Otorite kullanıcı ile aynı oturum anahtarın sahip olduğunu M_2 değerini kullanıcıya göndererek ispatlar (denklem 3.45).

$$M_2 = H(A, M_1, K) \tag{3.45}$$

4. UGULANABİLİR BİR SEÇİM PROTOKOLÜNÜN GERÇEKLENMESİ

Bu bölümde; bölüm 2.1 ‘de anlatılan gereksinimleri karşılayacak çok adaylı bir seçim sistemi tasarımı yapılmaktadır. Tasarım için Damg°ard ve Jurik [41]’ in evet/hayır oylama modeli esas alınmaktadır. Bu modelin, çalışmada anlatılan haliyle, neden uygulanabilir (güvenilir) olmadığı incelenmektedir.

4.1. Damg°ard - Jurik Evet / Hayır Oylama Modeli

Damg°ard ve Jurik bu modelde evet/hayır şeklinde bir oylamanın güvenilir bir şekilde nasıl yapıldığını göstermektedir.

1. Her kullanıcı kullanacağı v_i oyuna (0 yada1) karar verir ve r_i rasgele seçilmek üzere oyu açık seçim anahtarı (*election public key*) kullanarak Paillier kripto sistemine göre şifreler (denklem 4.1).

$$E_i = E(v_i, r_i) \tag{4.1}$$

2. Eğer şifrelenen oy 0 ise şifreleme ifadesi denklem 4.2 gibi, 1 ise denklem 4.3’deki gibi gösterilir.

$$E_i = g^0 r^n \bmod n^2 = r^n \bmod n^2 \tag{4.2}$$

$$E_i = g^1 r^n \bmod n^2 = g r^n \bmod n^2 \tag{4.3}$$

3. Kullanıcı oyun geçerliliğini göstermek için E_i veya E_i / g değerlerinden birinin Paillier kripto sisteme göre n. dereceden üs olduğunu ispatlar (bölüm 3.4.3). Buna göre, kullanıcı oyu 0 veya 1 olduğu sürece ispat geçerlidir.
4. Kullanıcı kullandığı şifreli oyu ve ispatını seçim panosuna yazar. Seçimi gözlemleyen herkes oyun geçerli olup olmadığını sınayabilir.
5. Seçim sonunda geçerli oyların çarpımı seçim sonucunu belirler (denklem 4.4).

$$\prod_i E_i = E(\sum_i v_i) \tag{4.4}$$

Damg°ard ve Jurik bu model ile çok adaylı bir seçim sisteminin yapılabileceğini göstermiştir. Bu modele göre, oy kullanıcısı L adaydan en fazla biri için evet(1) oyu kullanabilir. Kullanıcı isterse tüm adaylar için hayır(0) oyu kullanarak seçim için adayının olmadığı ve boş bir oy kullandığını gösterir. Kullanıcı her şifreli oy için oyun geçerli olduğunu gösteren bir ispat göndermek zorundadır.

4.2. Damg°ard - Jurik Modelinin Eksikleri

Bu model evet/hayır seçim için güvenilir olması yanında çok adaylı seçim sistemi için önerilen şekliyle uygulanabilir değildir. Bu yaklaşım ile tasarlanacak bir seçim sistemi bölüm 2.1 'de anlatılan seçim gereksinimlerini önemli ölçüde karşılamalıdır. Bu modelin temel eksikleri şunlardır:

1. Kullanıcının hangi aday için hangi oyu kullandığı bilgisi mevcut değildir. Bu sebeple sahtekâr bir otorite aday numaralarına göre sıralanmış şifreli oyları karıştırabilir. Kullanıcı, hangi oyu hangi aday için kullandığını açık olarak söylese bile oyları toplayan otorite bu bilgileri istediği şekilde değiştirebilir.

Bu gereksinimi dikkate alarak, oy ile aday numaraları arasında değiştirilemez bir ilişki kurulmalıdır.

2. Oyların seçim sürecinde kullanılıp kullanılmadığını gösteren bir zaman bilgisi (*time stamp*) mevcut değildir. Zaman bilgisi seçim otoriteleri tarafından üretilmiş olmalı ve seçim sona erdikten sonra kullanılan oylar geçersiz sayılmalıdır.
3. Sahtekâr otoritelerin seçim süresi sona ermeden az önce oylamaya katılmayan kullanıcıların yerine oy kullanması önlenemez. Oylamaya katılımın %100 olmadığı düşünülürse açık kalan oyların sahtekâr otoriteler tarafından kullanılması seçim sonuçlarını beklenmedik yönde etkileyebilir. Bu yüzden seçimi dışarıdan gözlemleyen biri, kullanıcının oyu kullanıp kullanmadığını doğrulayabilmelidir.

4.3. Önerilen Çok Adaylı Seçim Sistemi

Bu bölümde; Damg°ard - Jurik oylama modelini temel alan yeni bir seçim sistemi önerilmektedir. Önerilen seçim sistemi temel modelin eksiklerini (bölüm 4.2) kapatarak daha güvenilir bir seçim sistemi kurmayı hedefler. Bu çalışma ile ilk defa sahte oy kullanımının ZKP temelli kimlik doğrulama bilgileri ile nasıl önlenebileceği gösterilmektedir.

Önerilen bu yeni seçim sitemi aşağıdaki gibi çalışmaktadır:

1. Seçim başlamadan kullanıcılar SRP protokolü ile şifrelerini (*P*) belirler. Otoriteler ise kullanıcı şifresini doğrulamak için doğrulama bilgileri (*password verifier*) üretirler (bölüm 3.5.1). Otoriteler ayrıca dağıtık anahtar üretim protokolüyle seçimin gizli anahtarını aralarında paylaşırlar (bölüm 3.3).

2. Seçim başladığında kullanıcı gizli şifresini kullanarak SRP protokolü ile kimliğini doğrulatır.
3. Otoriteler kimliği doğrulanan her kullanıcı için bir zaman bilgisi (*T*) üretirler. Bu bilgi otoriteler tarafından dağıtık bir şekilde imzalanır (*S(T)*) ve kullanıcıya gönderilir. Bu bilgi sayesinde kullanıcı geçerli bir zaman diliminde oy kullandığını ispatlar. Bu bilgi boş bir oy pusulası olarak da düşünülebilir.
4. L adaylı bir seçim sisteminde kullanıcı seçtiği aday için evet (1), diğer adaylar için hayır (0) oyunu şifreler (denklem 4.5). Şifrelediği her ifadenin {0, 1} kümesinde seçildiğini göstermek için E_i veya E_i / g değerlerinden birinin Paillier kripto sisteme göre n. dereceden üs olduğunu ispatlar (denklem 4.6).

$$E_1 = E(v_1, r_1),\ E_2 = E(v_2, r_2),\ \ldots,\ E_L = E(v_L, r_L) \tag{4.5}$$

$$P_1 = \mathrm{Pr}\,oof(E_1),\ P_2 = \mathrm{Pr}\,oof(E_2),\ \ldots,\ P_L = \mathrm{Pr}\,oof(E_L) \tag{4.6}$$

5. *H* tek yönlü bir özet fonksiyonu olmak üzere; kullanıcı hangi şifreli oyu hangi aday için kullandığını göstermek için oy ispatı (P_i) ve aday numarasından (L_i) bir özet (λ_i) oluşturur (denklem 4.7). Bu sayede sahtekâr bir otoritenin oyların sırasını karıştırması veya yeni bir değer ile değiştirmesi önlenmiş olur.

$$\lambda_i = H(P_i, L_i) \tag{4.7}$$

P_i değeri oyun ispatı olup değiştirilemez olduğundan, bu değerin kullanımı son derece güvenlidir. Bu değer dışında kullanılacak bir değer sahtekâr bir otoritenin oy üzerinde değişiklik yapabilmesine izin verir.

6. Kullanıcı oyları kendisinin kullandığını göstermek için rasgele bir *r'* seçer ve kullanıcı şifresini (*P*) açık seçim anahtarı ile şifreler (denklem 4.8).

$$P' = E(P, r') \tag{4.8}$$

7. Kullanıcı son olarak $T, T(S), P'$ değerleri ile her aday için E_i, P_i, L_i, λ_i değerlerini seçim otoritesine gönderir. Otorite gelen değerleri seçim panosunda yayınlar.
8. Seçim süresi sona erdiğinde oyların sayımına başlanır. Sayım otoriteleri ilk olarak oyların zaman bilgisini kontrol ederler. Geçersiz bir zaman diliminde kullanılmış oylar, tüm otoritelerin katılımıyla dağıtık bir şekilde imzalanmamış olacağından geçersiz kabul edilir. Zaman bilgisi seçimin gizli anahtarı kullanılarak imzalandığından, sistem güvenlik parametresi t olmak üzere, t ve t' den küçük sayıda otorite tarafından değiştirilemez.
9. Otoriteler şifrelenmiş kullanıcı şifresini dağıtık bir şekilde çözer (bölüm 3.3) ve kullanıcıya ait SRP doğrulama bilgisi ile test ederler. Bu sayede elektronik oyun kullanıcı tarafından üretildiği doğrulanır. Aksi takdirde oy başkası tarafından üretilmiş sayılır ve geçersizdir.
10. Her kullanıcının en fazla bir aday için evet oyu kullanıp kullanmadığını test etmek için kullanıcının kullandığı tüm oylar çarpılır ve çarpım sonucu gizli seçim anahtarı ile çözülür (denklem 4.9). Çözüm sonucu 1 veya 0 ise kullanıcı en fazla bir aday için evet oyu kullanmıştır (Paillier homomorfizmi).

$$\prod_{j}^{L} E_{i,j} = E(\sum_{j}^{L} v_{i,j}) \in \{0,1\} \tag{4.9}$$

Boş oy (tüm adaylar için hayır) kullanımının izin verildiği seçim sistemlerinde işlem sonucu sıfır ise kullanıcının hiç bir adayının olmadığı otoriteler tarafından bilinebilir. Bu bilgi seçimin gizlilik prensibini ihlal edeceğinden, bu adım yalnızca tek adaylı seçim sistemlerinde uygulanabilir.

11. Kullanıcının hangi aday için hangi oyu kullandığı λ_i özet bilgisi ile doğrulanır. Her adayın oyu ayrılarak sayılır ve seçim panosunda yayınlanır.

4.4. Önerilen Sistemin Ölçülmesi

Tasarımı yapılmış bir seçim sisteminin ölçülebilir olması için elektronik seçim sisteminin gereksinimlerini ne ölçüde karşıladığı incelenmelidir. Bölüm 2.1'de tanımlamaları yapılmış bu gereksinimlerin önerilen sistem ile ne ölçüde karşılandığı bu bölümde incelenecektir.

- *Yetki:* Yetki kontrolü SRP protokolü ile gerçekleştirilir. Yalnızca otorite tarafında doğrulama bilgisi tanımlı kullanıcılar oy kullanabilir. Doğrulama tek taraflı olabileceği gibi, sunucu ve kullanıcı aynı oturum için birbirlerinin kimliklerini doğrulayabilirler.
- *Gizlilik:* Önerilen sistemde seçim sonucu oyların içerikleri açılmadan belirlenir ve tüm oyların çarpımının çözülmesi şeklinde hesaplanır. Seçim gizli anahtarı otoriteler arasında güvenli anahtar dağıtım protokolü ile paylaştırılmıştır. Güvenlik parametresi t olan bir seçim sisteminde ancak t+1 hilekâr otoritenin koalisyonu ile anahtar bir araya getirilebilir. Güvenlik parametresi iyi seçildiği sürece kullanıcı ve oy arasında ilişki kurmak olanaksızdır.
- *Kullanıcı tarafından doğrulama:* Şifrelenmiş şekilde gönderilen kullanıcı şifresi mesaj panosunda yayınlanır. Kullanıcı bu ifadeyi tekrar üretebilir ve bu sayede oyun sahtesiyle değiştirilip değiştirilmediğini doğrulayabilir. Şifreli ifadenin üretilmesi için kullanılan *r'* değeri (denklem 4.9) doğrulama amaçlı kullanıcı tarafından saklanmalıdır. Bu sayede kullanıcı aynı şifre için aynı şifreli değeri tekrar üretebilir ve eşitliğini test edebilir. Saklanan değer

ile kullanılan oy arasında hiçbir ilişki kurulamayacağından bu değer bir oy reçetesi olarak algılanmamalıdır.

- *Herkes tarafından doğrulama:* Kullanıcıların gönderdikleri oy bilgileri seçim panosunda yayınlanır. Bu yüzden seçim süreci herkes tarafında izlenebilir ve otoritelerin adil davranıp davranmadıklarına karar verilebilir. Örneğin; süreci dışarıdan izleyen bir gözlemci kullanıcının hangi aday için hangi şifreli oyu kullandığını doğrulayabilir ve yapılan hileyi diğer seçim otoritelerine bildirebilir. Seçim sürecinin bu ölçüde şeffaf olabilmesini sağlamak ancak seçim anahtarının otoriteler arasında gizli kalmasıyla mümkündür.
- *Doğruluk***:** Katılımcılar oyların sayımından önce seçim sonucu hakkında kısmi bilgiye sahip değillerdir. Bunun olabilmesi için *t+1* sahtekâr otoritenin bir araya gelerek gizli anahtarı üretmesi ve seçimin kısmi sonucunu çözmesi gerekir.
- *Sağlamlık***:** Seçim sürecini bozmak veya aksatmak için yapılacak girişimler seçim sürecini etkileyemez, çünkü seçim sistemi herkese açıktır ve yapılan işlemler herkes tarafından doğrulanabilir. Seçim sürecinin her adımında ispat yöntemlerinden yaralanıldığından yapılan sahtekârlıklar oy kullanıcıları veya seçimi izleyen üçüncü şahıslar tarafından ortaya çıkarılabilir.
- *Reçetesiz oy kullanımı***:** Önerilen seçim sistemi herkese açık ve herkes tarafından doğrulanabilir olduğundan oy reçetesine gerek duyulmaz. Ayrıca oy reçeteleri üçüncü şahısların kullanıcı oyu hakkında bilgi sahibi olmasına ve kullanıcıyı belli adaya oy vermesi için zorlamasına sebep olabileceğinden kullanımları sakıncalıdır.

5. SONUÇ

Bu çalışmada; Paillier homomorfizmi üzerine kurulu, elektronik seçim sisteminin gereksinimlerini tam olarak karşılayan yeni bir seçim sistemi önerilmektedir. Önerilen sistem Damg°ard - Jurik oylama modelini esas almakta ve bu modelin eksik kaldığı noktaları çözmektedir.

Çalışmada ilk defa ZKP temelli SRP protokolü ile sahte oy kullanımının nasıl önlenebileceği gösterilmektedir. Bu sayede sahtekâr otoritelerin veya üçüncü şahısların kullanıcı adına sahte oy kullanmaları önlenmiş olur. Kullanıcı SRP şifresi ile tüm oy bilgisinin özetini oluşturarak bilginin en son kullanıcı tarafından üretildiğini ispatlayabilir.

Önerilen sistem yardımıyla kullanıcı hangi oyu hangi aday için kullandığını güvenilir bir yolla seçim otoritelerine gösterebilir. Bu, temel alınan modelde eksik bırakılmış bir özelliktir. Bunu yaparken ZKP ispat bilgilerinden yararlanılmıştır.

Seçim öncesi veya sonrası oy kullanımını engellemek için zaman bilgisinin eşik değerli ve dağıtık bir şekilde Paillier kripto sistemi ile şifrelenmesi ve bu bilginin boş oy pusulası olarak kullanımı seçim sürecinin güvenirliğini sağlayacak diğer bir yeniliktir.

5.1. İleriki Çalışmalar

Önerilen sistemde her aday için farklı şifreli ifadeler ve ispat bilgileri üretilmektedir. Bu, oy bilgisinin büyümesine ve oy sayımının uzamasına neden olmaktadır. Daha etkin bir seçim sistemi ancak oyun sayım sürecini hızlandıracak

şekilde kodlanmasıyla mümkündür. Yeni tasarlanacak elektronik seçim sistemleri bu ihtiyacı karşılayacak şekilde tasarlanacaktır.

KAYNAKLAR

[1] Chaum D. L., "Untraceable electronic mail, return address, and digital pseudonym", Communication of ACM, volume:24, number:2, Newyork, 1981.

[2] Chaum D., "Blind signatures for untraceable payments", Crypto'82, pages: 199–203, Newyork, 1983.

[3] http://www.technologyreview.com/articles/04/09/ap 092604.asp, (01/04/2006).

[4] http://www.cybervote.com, (20.05.2006)

[5] Okamoto T., "Receipt-free electronic voting schemes for large scale elections", Proceedings of the 5th International Workshop on Security Protocols, Springer-Verlag, LNCS 1361, pages:25-35, Paris, 1997.

[6] Benaloh J., "Verifiable Secret-Ballot Elections", Yale University, Department of Computer Science, PhD thesis, New Haven, CT, September 1987.

[7] Kiayias A., Yung M., "The Vector-Ballot e-Voting Approach", Financial Cryptography 8th International Conference, Springer-Verlag, LNCS 3110, pages:72-89, 2004.

[8] Park C., Itoh K., Kurosawa K., "All-nothing election scheme and anonymous channel", EUROCRYPT '93, Springer-Verlag, LNCS 765, pages: 248–259, 1994.

[9] Pfitzmann B., "Breaking an efficient anonymous channel", EUROCRYPT '94, Springer-Verlag, LNCS 950, pages:332–340, Perugia, Italy, 1995.

[10] Michels M., Horster P., “Some remarks on a receipt-free and universally verifiable mix-type voting scheme”, ASIACRYP ’94, Springer-Verlag, LNCS 1163, pages:125–132, 1996.

[11] Abe M., “Universally verifiable mix-net with verification work independent of the number of mix-servers”, EUROCRYPT ’98, Springer-Verlag, LNCS 1403, pages:437–447, 1998.

[12] Hirt M., Sako K., “Efficient receipt-free voting based on homomorphic encryption”, EUROCRYPT ’00, Springer-Verlag, LNCS 1807, pages:539–556, 2000.

[13] Magkos E., Burmester M., Chrissikopoulos V., “Receipt-freeness in largescale elections without untappable channels”, Proceedings of the IFIP Conference on Towards The E-Society: E-Commerce, E-Business, E-Government, volume:202, pages:683–694, 2001.

[14] Lee B., Boyd C., Dawson E., Kim K., Yang J., Yoo S., **“**Providing Receipt-freeness in Mixnet-based Voting Protocols”, Springer-Verlag, LNCS 2971, pages:245-258, 2003.

[15] Chaum D., Fiat A., Naor M., “Untraceable electronic cash”, Springer-Verlag, LNCS 403, pages:319–327, 1990.

[16] Radu C., Govaerts R., Vanderwalle J., “A restrictive blind signature scheme with applications to electronic cash”, Communications and Multimedia Security II , pages:196–207, Chapman & Hall, London, 1996.

[17] Lysyanskaya A., Ramzan Z., “Group blind digital signatures: A scalable solution to electronic cash”, Financial Cryptology (FC ‘98), Springer-Verlag, LNCS 1465, pages:184-197, 1998.

[18] Bleumer G., “Secure PC-franking for everyone”, Electronic Commerce and Web Technologies (EC-Web 2000), Springer-Verlag, LNCS 1875, pages:94-109, 2000.

[19] Kim S., Oh H., “A New Electronic Check System with Reusable Refunds”, International Journal of Information Security, volume:1, number:3, pages:175-188, 2002.

[20] Fujioka A., Okamoto T., Ohta K., “A practical secret voting scheme for large scale elections”, AUSCRYPT ’92, Springer-Verlag, LNCS 718, pages:244–251, 1992.

[21] Horster P., Michels M., Petersen H., “Blind multisignature schemes and their relevance to electronic voting”, Proc. 11th Annual Computer Security Applications Conference, pages:149–156, Gaithersburg, 1995.

[22] Okamoto T., “Receipt-free electronic voting schemes for large scale elections”, In Proc. of Workshop on Security Protocols '97, Springer-Verlag, LNCS 1361, pages:25–35, 1997.

[23] Cranor L., Cytron R., “Sensus: A security-conscious electronic polling system for the Internet”, In Proceedings of the Hawaii International Conference on System Sciences, Hawaii, January, 1997.

[24] Ohkubo M., Miura F., Abe M., Fujioka A., Okamoto T., "An improvement on a practical secret voting scheme", ISW '99, Spring-Verlag, LNCS 1729, pages:225–234, London, 1999.

[25] Camenisch J.L., Piveteau J. M., Stadler M. A., "Blind signatures based on the discrete logarithm problem", Springer-Verlag, LNC 950, pages:428-432, 1994.

[26] Paillier P., "Public-Key Cryptosystems based on Composite Degree Residue Classes", Proceedings of EUROCRYPT '99, Springer Verlag, LNCS 1592, pages:223-238, 1999.

[27] Cramer R., Gennaro R., Schoenmakers B., "A secure and optimally efficient multi-authority election scheme", EUROCRYPT '97, Springer-Verlag, LNCS 1233, pages:103–118, 1997.

[28] Benaloh J. C., Tuinstra D., "Receipt-free secret-ballot elections (extended abstract)", Proc. 26th ACM Symposium on the Theory of Computing (STOC), pages:544-553, 1994.

[29] Sako K., Kilian J., "Secure voting using partial compatible homomorphisms", CRYPTO '94, Springer-Verlag, LNCS 839, pages:248–259, 1994.

[30] Cramer R., Franklin M., Schoenmakers B., Yung M., "Multi-authority secretballot elections with linear work", EUROCRYPT '96, Springer-Verlag, LNCS 1070, pages:72–83, 1996.

[31] Baudron O., Fouque P., Pointcheval D., Poupard G., Stern J., "Practical multi-candidate election system", Annual ACM Symposium on Principles of Distributed Computing, pages:274–283, Newport, 2001.

[32] Lee B., Kim K., “Receipt-free electronic voting scheme with a tamperresistant randomizer”, ICISC2002, pages:405–422, 2002.

[33] Damg°ard I., Jurik M., “A generalisation, a simplification and some applications of paillier’s probabilistic public-key system”, In Public Key Cryptography ’01, Springer-Verlag, LNCS 1992, pages:119–136, 2001.

[34] Damg°ard I., Jurik M., Nielsen J. B., “A generalization of paillier’s public-key system with applications to electronic voting”, Springer-Verlag, pages:467-482, 2005.

[35] Shamir A., “How to share a secret”, In Communications of the ACM, ACM Press, volume:22, number:11, pages:612-613, November 1979.

[36] Schoenmakers B., “A simple publicly verifiable secret sharing scheme and its application to electronic voting”, CRYPTO ’99, Springer-Verlag, LNCS 1666, pages:148–164, 1999.

[37] Shoup V., “Practical Threshold Signatures”, Proceedings of EuroCrypt 2000, Springer Verlag, LNCS 1807, 2000.

[38] Pedersen T. P., “Non-interactive and information-theoretic secure verifiable secret sharing”, CRYPTO 91, pages:129–140, 1992.

[39] Frankel Y., MacKenzie P. D., Yung M., “Robust Efficient Distributed RSA-Key Generation”, Proc. of STOC 98, pages:663-672, 1998.

[40] Damg°ard I., Koprowski M., “Practical threshold RSA signatures without a trusted dealer”, EUROCRYPT ‘01, Springer Verlag, LNCS 2045, pages:152-165, 2001.

[41] Damg°ard I., Jurik M., “Efficient protocols based on probabilistic encryption using composite degree residue classes”, Cryptology ePrint Archive, Report 2000/008, 2000.

[42] Fiat A., Shamir A., “How to Prove Yourself: practical solutions of identification and signature problems”, CRYPTO ’86, Springer-Verlag, LNCS 263, pages:186-194, 1987.

[43] http://gost.isi.edu/publications/kerberos-neuman-tso.html, (29.12.2006)

[44] Bellovin S. M., Merritt M., “Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks”, In Proceedings of the I.E.E.E. Symposium on Research in Security and Privacy, pages:, 72-84, Oakland ,1992.

[45] Bellovin S. M., Merritt M., “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, ACM Press, 1993.

[46] Wu T., “The Secure Remote Password Protocol”, In Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium, pages:97-111, San Diego, CA, Mar 1998.

ÖZGEÇMİŞ

Lisans eğitimini Yıldız Teknik Üniversitesi bilgisayar mühendisliği bölümünde tamamlamıştır. Lisansüstü eğitimi halen Maltepe Üniversitesi bilgisayar mühendisliği bölümünde devam etmektedir. Temel ilgi alanları veri güvenliği ve kriptolojidir. İstanbul da bir yazılım firmasında Java teknolojileri üzerine yazılım geliştirmektedir.