İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

ETMENLERLE ELEKTRONİK OYLAMA

YÜKSEK LİSANS TEZİ

Müh. Mehmet Tahir SANDIKKAYA

Anabilim Dalı: MÜHENDİSLİKTE İLERİ TEKNOLOJİLER

Programı: BİLGİSAYAR BİLİMLERİ

EYLÜL 2005

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

ETMENLERLE ELEKTRONİK OYLAMA

YÜKSEK LİSANS TEZİ
Müh. Mehmet Tahir SANDIKKAYA
704021003

Tezin Enstitüye Verildiği Tarih : 2 Haziran 2005
Tezin Savunulduğu Tarih : 2 Eylül 2005

Tez Danışmanı : Prof.Dr. Bülent ÖRENCİK
Diğer Jüri Üyeleri Prof.Dr. Nadia ERDOĞAN
Prof.Dr. Oya KALIPSIZ (Y.T.Ü.)

EYLÜL 2005

ÖNSÖZ

Yüksek lisans eğitimim boyunca yardımını eksik etmeyen, tezimi hazırlarken karşılaştığım en zor engelleri yerinde yönlendirmelerle aşmamı sağlayan, görüşleriyle konuya bakışımı ve yaklaşımımı genişleten danışmanım sayın Prof. Dr. Bülent ÖRENCİK'in kattıklarıyla bu metin tamamlanmıştır. Eğitim hayatımı yönlendiren ve dolayısıyla bu metne katkısı olan tüm öğretmenlerime, aileme, arkadaşlarıma; bunca iyiliğin karşılığında; ancak teşekkür edebiliyorum.

Mehmet Tahir SANDIKKAYA

Eylül 2005

İÇİNDEKİLER

TABLO LİSTESİ

ŞEKİL LİSTESİ

ÖZET

Seksenli yılların sonunda ortaya çıkan şifrebilimsel kanıtlama yöntemleriyle birlikte, temel olarak, eşişlemli şifreyazım tabanlı, karıştırıcı ağ tabanlı ve körleştirme tabanlı olmak üzere üç kümeye ayrılabilecek birçok elektronik oylama dizgesi geliştirilmiştir. Tüm bu yaklaşımların ortak noktası, hepsinin gerçek zamanda sunucu tarafında işlem yapma zorunluluğudur. Bu sorunu ortadan kaldıracak bir dizgenin tasarımı elektronik oylamayı ucuzlatacaktır.

Etmen tabanlı yaklaşımla tasarlanmış bilinen bir elektronik oylama dizgesi yoktur. Etmen tabanlı bir yaklaşımın getirileri dizgeyi özelleştirilebilir, değiştirilebilir ve esnek kılmak; bunun yanında hesap yükünü dağıtmak olabilir.

Bu öngörülerden yola çıkarak, sunucu tarafında gerçek zamanda hesaplama gerektirmeyen etmen tabanlı iki elektronik oylama dizgesi önerilmiştir. Bu iki dizgede alışıldık şifrebilimsel yöntemleri kullanan ikişer etmen kullanılmıştır. Bu etmenlerin biri oy bilgisini işlerken diğeri seçmen bilgisini işleyecektir. Etmenlerin birlikte çalışmasıyla seçmenlerin oyları toplanabilir ve sayılabilir.

Önerilen dizgelerde elektronik oylama dizgelerinin sağlaması gereken koşullardan bazıları şifrebilimsel yöntemlerle oluşturulurken, bazıları da dizgelerin işleyişi içinde oluşturulur. Oluşturulan dizgeler kullanılan şifrebilimsel yöntemlerin ve etmenlerin güvenli olduğu varsayımıyla güvenli görünmektedir. Bununla birlikte, yöntemlerin ve etmenlerin güvenliği de çalışmada tartışılacaktır.

Bu çalışmada önerilen dizgeler açıklanmış ve var olan dizgelerle kıyaslanmışlardır. Sonuçta, beklentilere uygun etmen tabanlı dizgelerin geliştirilebileceği görülmüştür. Dizgelerin benzetimleri kişisel bilgisayarlarda yapılmış, ayrıca olurlukları irdelenmiştir.

SUMMARY

Many electronic voting systems, classified mainly as homomorphic cryptography based, mix-net based and blind signature based, appear after the eighties when zero knowledge proofs were firstly introduced. The common ground for all these three systems is the fact that none of them works without real time cryptologic calculations that should be held on a server. A design that redeem this issue can decrease the cost of electronic voting.

As far as known, the agent-based approach has not been used in a secure electronic voting system. Advantages of the agent-based approach are not only the ease of creating a system that can be easily modified and customized, but also a widely distributed computation load.

In this study, two agent-based electronic voting schemas, which does not contain real time calculations on the server side, are proposed. Each schema contains two agents that are using conventional cryptologic methods. One of the agents processes the vote while the other recognizes the voter. By the cooperation of these two agents, votes can be collected for tallying.

Some of the requirements of an electronic voting system are constructed by the cryptologic methods and some of them constructed within the schema's mechanism. The schemas seems quite secure if the used cryptologic methods and agents are secure. However, security of the agents will be discussed in the study.

In this study, proposed schemas will be explained and compared with already known electronic voting systems. As a result, it can be said that it is possible to create the desired agent-based electronic voting system. Schemas are simulated in a personal computer and the feasibility of the schemas are investigated.

1 GİRİŞ

İnsanlığın yüzyıllar içinde geliştirdiği yönetim biçimleri içinde, en azından günümüzde, en önemli görüneni demokrasidir. Günümüzde yaygın olarak uygulayabildiğimiz temsilî demokrasinin günün birinde doğrudan demokrasiye dönüşmesi umulabilir. Bunun gerçekleşeceğini varsaydığımızda, şu an elimizde bulunan en önemli aracın bilişim teknolojisi olduğu açıklıkla görülecektir. Var olan ya da oluşturulacak elektronik oylama yöntemleri günümüzdeki temsilî demokrasinin gereklerini karşılayabileceği gibi, gelecekteki olası doğrudan demokrasi oluşumlarının da temelini oluşturabilir. Elektronik oylama konusundaki araştırmaların hem bugün hem de gelecekte yararlı olacağını düşündüren bu yorumla konunun ele alındığı bu çalışmada var olan yöntemlere farklı bir bakışla yeni bir yöntem önerilecek ve önerilen yöntem en sade biçimiyle gerçeklenerek diğer yöntemlerle kıyaslanacaktır.

Hemen hemen tüm elektronik oylama yöntemlerinin iddiası alışıldık oylama yöntemlerinin yerine geçmek, hatta onlardan daha verimli işlemektir[1]. En başta, bir oylamanın herhangi bir aşamasının insansızlaştırılmasının hile olasılığını azaltacağı varsayımıyla elektronik oylamanın olağan oylamadan daha güvenli olduğu söylenebilir. Elektronik oylamanın alışıldık oylamaya göre bir başka üstün yanı ucuzluğudur. Elektronik oylama yöntemleri sadece veriyi saklayacak ortamlara gerek duyacağından, alışıldık yöntemlerdeki kırtasiye, posta, ve çalışan giderlerinin önüne geçilmesi sağlanabilir. Elektronik oylamanın bir başka önemli getirisi, sayımın hızla sonuçlandırılmasıdır. Alışıldık yöntemlerdeki sayım görevlilerinin yerini alan bilgisayarlar sayımı hem insan faktöründen arındırarak hatasızlaştırmakta, hem de birkaç saat içinde kesin sonuçların açıklanmasına yetecek kadar hızlandırmaktadır.

Seksenli yılların sonunda ortaya çıkan[2] şifrebilimsel kanıtlama yöntemleriyle birlikte doğan elektronik oylama düşüncesinin geniş bir uygulama alanı vardır. Belki de bu nedenle, elektronik oylama için bugüne kadar önerilen çok sayıda dizge vardır. Dizgeler, üç ana başlık altında toplanabilir: karıştırıcı ağ tabanlı dizgeler (mix-net), eşişlemli şifreyazım (homomorphic cryptography) tabanlı dizgeler ve körleştirme (blinding) tabanlı dizgeler[3]. Karıştırıcı ağ tabanlı dizgelerde sayım yetkisine sahip

yetkeler oyları ya da oy kümelerini kendi aralarında rastgele yollarla taşıyarak seçmenden bağımsızlaştırırlar. Eşişlemli dizgelerde tüm oylar eşişlemli şifreyazım kullanılarak aynı veri paketinin içinde toplanır. Bu paketin şifresinin tek seferde çözülmesiyle oylama sonucuna ulaşılır. Körleştirme tabanlı dizgelerde ise, seçmenlerin kullandıkları oylar bir körleştirme çarpanıyla gizlenerek yetkeye onaylatılır ve sayım yetkesine gönderilir.

Bu üç temel yaklaşımın birçok örneği varsa da, etmen tabanlı çevrimdışı bir yaklaşım bilinmemektedir. Çalışmada etmen tabanlı bir yaklaşımın elektronik oylama dizgelerine uygulanabilirliği tartışılacak; olası getirileri ve götürüleri belirlenmeye çalışılacaktır.

2 TEMELLER

Elektronik oylamanın anlaşılmasında yararlı olacak temel bilgiler bu bölümde kısaca anlatılacaktır. Çalışma içinde gerekli görülen yerlerde temel bilgiler derinleştirilerek önerilen yöntem ve uygulanışı açıklanacaktır.

2.1 Elektronik Oylama

Seçmenlerin kullandıkları oyların sayısal ortamda saklanıp sayıldığı dizgelere elektronik oylama dizgeleri denir. Bu dizgelerde kağıt ve mürekkebin yerini sayısal veriler alır. Elektronik oylama dizgeleri alışıldık dizgelere birçok konuda benzerdir. Aynı şekilde, seçmen gizliliğini, oyların kullanıldıktan sonra değiştirilememesini, sayımın hatasız ve doğru yapılmasını gerektirirler. Bu gereksinimler şifrebilimsel yöntemlerle karşılanır.

Elektronik oylama dizgelerini işleyişlerine göre iki sınıfa ayırmak yararlı olacaktır. Alışıldık oylamaya benzer biçimde, seçmenlerin bir seçim merkezîne giderek elektronik araçlar yardımıyla oy kullandıkları dizgeleri *merkezî elektronik oylama dizgeleri*; seçmenlerin diledikleri bir konağı kullanarak oy kullandıkları dizgeleri de *yaygın elektronik oylama dizgeleri* olarak adlandırmak uygundur.

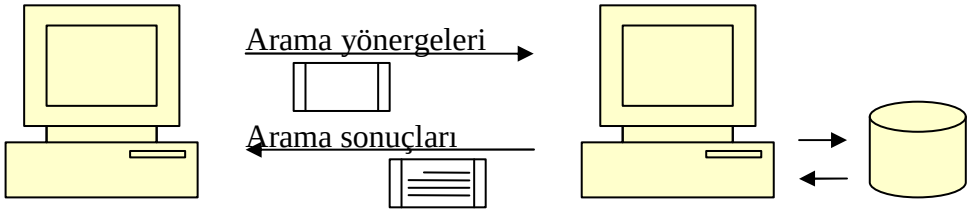
Bir başka sınıflandırma dizgelerin şifrebilimsel yöntemleri kullandıkları zamanlar düşünülerek yapılabilir. Oylama süresince şifrebilimsel hesapların yapılmasını gerektiren dizgelere *çevrimiçi elektronik oylama dizgeleri*; oylama süresince şifrebilimsel hesaplama yapılmasını gerektirmeyen dizgelere de *çevrimdışı elektronik oylama dizgeleri* denilebilir.

Son zamanlarda gerçekleştirilmiş az sayıdaki geniş çaplı elektronik oylama arasında başarılı sayılabilecek örnekler vardır. 2004 yılındaki Amerika Birleşik Devletleri başkanlık seçimleri örnek bir uygulama olarak düşünülebilir. Bizim adlandırmamızla merkezî çevrimiçi elektronik oylama dizgesi olarak sınıflandırılabilecek olan oylama sırasında sayısal araçlarla oylar saklanmış, yanı sıra alışıldık yollarla oylama gerçekleştirilmiştir. Kısaca, alışıldık oylama ile elektronik oylama birbirini

tamamlayan iki unsur olarak görülmüştür. Böyle bir güvenceye rağmen, bu örneğe yöneltilen ciddi eleştiriler vardır. Eleştirilerin odağında ise insanî ve kanunî yetersizlikler göze çarpsa da aslında üstesinden gelinebilecek teknolojik yetersizlikler de görülür[4].

2.2 Etmen Tabanlı Yaklaşım

Tanımı tartışılıyor olsa da genel bir etmenin tanımını vermek yararlı olacaktır: "Bir işlemler kümesini kullanıcının ya da bir başka uygulamanın yerine belirlenen bağımsızlık ya da benzerlik çerçevesinde gerçekleştiren ve kullanıcının amacı ya da isteği doğrultusunda bilgi veren yazılım parçası." Bir başka bilgisayarda tutulan veritabanında arama yapması için tasarlanan etmenin şematik anlatımı **Şekil 2.1**'de görülebilir. Oluşturulan etmen ikinci bilgisayara göç etmiş, üzerinde taşıdığı yönergeleri birinci bilgisayarın bir uzantısı gibi orada çalıştırarak sonuçları almış ve kaynağı olan bilgisayara geri dönmüştür. Sunucu istemci yaklaşımından farklı olarak etmen tabanlı yaklaşımda veriyi paylaşan tarafın (sunucunun) farklı sorgulamalar için farklı işlevler barındırma zorunluluğu kalmamış, işlevin geliştirilmesi diğer tarafa bırakılmıştır. Etmenlerin bir görev üstlenerek bir çok farklı bilgisayarı dolaşması, her bilgisayardan gerekli verileri toplayarak kaynak bilgisayara dönmesi de olasıdır. Böylece veri toplamak isteyen bilgisayar istemci sunucu yaklaşımındaki gibi her bir bilgisayardan yanıt beklemek zorunda kalmayacak, yanıtlar toplandığında bundan haberdar olacaktır.



Şekil 2.1 Bir etmenin başka bir bilgisayarın veritabanında arama yapması

Daha belirleyici olması için çalışmada sözü edilen etmenlerin tanımı da yapılmalıdır: "Oylamada yer alan tarafların çalıştırmakla yükümlü olduğu yönergeleri onların adına, bir başka tarafın kaynaklarını kullanarak, çalıştıran yazılım parçaları."

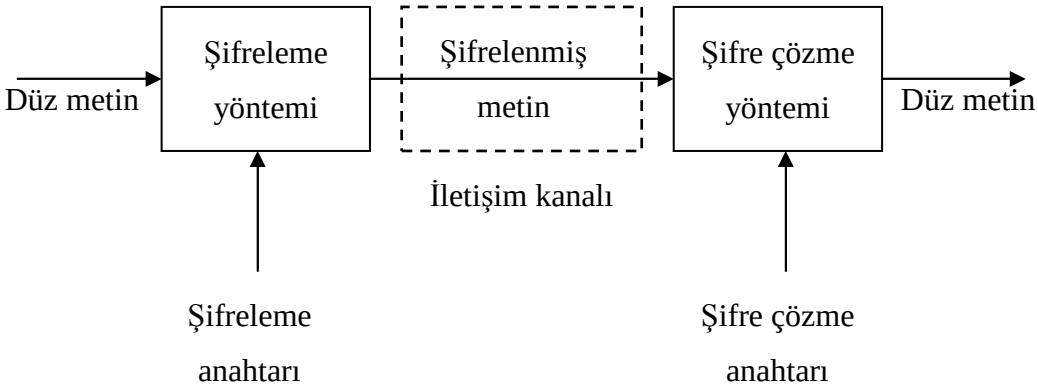
2.3 Şifreyazım

Türkçe'si "şifreyazım" olarak önerilen kriptografi eski Yunanca "kript" (gizli) ve "grafi" (yazım, çizim) sözcüklerinden türemiştir. Şifreyazım yüzyıllar boyu çeşitli amaçlarla kullanılmış ve geliştirilmiş, sonunda güncel karmaşık durumuna ulaşmıştır. İlkel şifreyazım yazıda kullanılan karakterlerin yerleri değiştirilerek ya da bir karakterin yerine bir başkası kullanılarak yapılmıştır. Günümüzde kullanılan ilkeler de aynı olmakla birlikte, değişen, yer değiştirmelerin ve yerine kullanımların şifre çözümlemeyi, yani şifrelenmiş metinden gerçek metnin elde edilmesini, olanaksızlaştıracak kadar karmaşıklaştırılmış olmasıdır. Genel şifreyazımın şematik anlatımının gösterildiği **Şekil 2.2**'de yazı boyunca kullanılacak terimler de görülebilir.

Şifreleme okunabiliri bir metinden gizli, şifrelenmiş bir metin oluşturmaya yarayan işlev olarak tanımlanabilir. Şifre çözme ise, şifrelemenin etkisini yok edecek bir ters işlev olarak tanımlanabilir.

Türkçe'si "Şifre çözümleme" olarak önerilen kriptanaliz ise şifre çözmeden farklı olarak şifrelenmiş metinden anahtarlara ya da şifre çözmeye yarayan diğer bilgiler olmadan düz metni oluşturma çabasıdır.

"Şifrebilim" olarak önerilen kriptoloji; şifreyazımı, şifre çözümlemeyi ve anlamını genişleterek gerçekte şifrelemeye ya da şifre çözmeye yaramayan ama bu işlemler sırasında yardımcı olan işlevleri de içeren geniş bir tanıma sahiptir.



Şekil 2.2 Şifreyazımın şematik anlatımı

Çalışmada bilinen şifrebilimsel yöntemler kullanılmaktadır. Kullanılan şifrebilimsel yöntemlerin bazıları iyi bilinen yöntemlerken bazıları bilinen yöntemlerin bir arada kullanılmasıyla ortaya çıkar. Bu nedenle, çalışmanın anlatımında gerekli görülen temel şifrebilimsel yöntemler burada kısaca açıklanacak, çalışmanın devamında, gerekli görülen yerlerde, bu açıklamalara çalışmaya özel durumlara ilişkin eklemeler yapılacaktır.

2.3.1 Bakışımlı Şifreyazım

Bakışımlı (symmetric) şifreyazımda düz metindeki harflerin yeri değiştirilerek ya da harfler farklı harflerle değiştirilerek şifrelenmiş metin elde edilir. Yer değiştirmeleri ve yerine koymaların hangi düzende yapılacağını belirleyen algoritma herkesçe bilinmesine rağmen hangi değişikliklerin yapılacağı anahtara bağlıdır. Bakışımlı şifreyazımda sözü geçen anahtar tektir, yani şifreleme anahtarı ile şifre çözme anahtarı aynıdır. İletişim kanalının herkesçe dinlenebilir olduğu varsayılırsa dizgenin güvenliğinin anahtarın güvenliğiyle eşdeğer olduğu görülecektir. Denklem (2.1)'de bakışımlı şifreleme ve bakışımlı şifre çözme işlevlerle anlatılmıştır. "DüzMetin", "Anahtar" parametresiyle "Şifreleme" işlevinden geçirildiğinde "ŞifrelenmişMetin" oluşmaktadır. Burada gösterilen "Şifreleme" ve "ŞifreÇözme" işlevleri herhangi bir algoritma kullanılarak gerçekleştirilmiş olabilir.

$$\begin{aligned} Şifreleme_{Anahtar}(DüzMetin) &= ŞifrelenmişMetin \\ ŞifreÇözme_{Anahtar}(ŞifrelenmişMetin) &= DüzMetin \end{aligned} \tag{2.1}$$

Benzer şekilde, "ŞifrelenmişMetin" yine aynı "Anahtar" parametresiyle "ŞifreÇözme" işlevinden geçirildiğinde "DüzMetin" yeniden elde edilmektedir.

2.3.2 Bakışımsız Şifreyazım

Bakışımsız (asymmetric) şifreyazımda iki ayrı anahtar kullanılır. İdeal durumda bu iki anahtardan birinin bilinmesiyle diğerini elde etmek olanaklı değildir. Anahtarlardan biriyle şifrelenen düz metin diğer anahtarın şifre çözmede kullanılmasıyla yeniden oluşturulabilir. Bu iki anahtar "açık anahtar" ve "gizli anahtar" olarak adlandırılırlar. Bu dizgenin güvenliği gizli anahtarın güvenliğine denktir. İletişim kuran taraflardan birinin kendine ilişkin gizli anahtarı koruduğu

varsayılırsa, açık anahtarı bilen diğer taraf ancak onun şifrelediği metinlerin şifresini çözebilecektir. Benzer şekilde, açık anahtara sahip olan taraf bu anahtarı kullanarak şifrelediği metinlerin şifresinin ancak gizli anahtara sahip biri tarafından çözüleceğinden emin olacaktır.

$$\begin{aligned} &Şifreleme_{GizliAnahtar}(DüzMetin) = ŞifrelenmişMetin \\ &ŞifreÇözme_{AçıkAnahtar}(ŞifrelenmişMetin) = DüzMetin \end{aligned} \tag{2.2}$$

$$\begin{aligned} &Şifreleme_{AçıkAnahtar}(DüzMetin) = ŞifrelenmişMetin \\ &ŞifreÇözme_{GizliAnahtar}(ŞifrelenmişMetin) = DüzMetin \end{aligned} \tag{2.3}$$

Denklem (2.2)'de gizli anahtara sahip olan tarafın gönderdiği metnin şifrelenmesi ve şifresinin çözülmesi işlevlerle gösterilirken, denklem (2.3)'de gizli anahtara sahip olan taraf gönderilen metinlerin şifrelenmesi ve şifresinin çözülmesi gösterilmiştir.

2.3.3 Öz alma

Öz alma (message digest, hash) bir metne ilişkin özet çıkarma işlemidir. Şifrebilimde kullanılan öz alma işlevleri her metin için aynı uzunlukta özler üretirler. Bir metin özü kullanılarak yeniden oluşturulamaz. İdeal şartlarda bu özlerin birbiriyle çakışmadığı varsayılır. Özlerin çakışması olasılığı, karakteristik olarak, özün uzunluğuyla belirlidir. Öz alma işlevi denklem (2.4)'te gösterilmiştir.

$$ÖzAlma(Metin) = Öz_{Metin} \tag{2.4}$$

2.3.4 İmzalama

Bir metnin özünün gizli anahtarla şifrelenmesiyle metin imzalanmış olur. Varsayımımızda her metnin tek bir özü olduğuna ve bu öz imzalayanın gizli anahtarıyla şifrelenmiş olduğuna göre, imzalayanın açık anahtarıyla şifreyi çözen biri şifreyi çözerek bulduğu öz ile metne ilişkin özü karşılaştırarak, metnin imzalayan tarafından kabul edilmiş metin olup olmadığını anlayabilir. Bu durumda, bir imzanın

güvenliği gizli anahtarın güvenliğine denktir. Denklem (2.5)'de imzalama işlevi gösterilmektedir.

$$İmzalama(Metin) = Şifreleme_{GizliAnahtar}(ÖzAlma(Metin)) = İmza_{Metin} \quad (2.5)$$

2.3.5 Körleştirme

Bir düz metnin uğradığı değişiklikleri şifrelenmiş metne, şifrelenmiş metnin uğradığı değişiklikleri düz metne aktarabilen şifrelemeye körleştirme (blinding) denir[6]. Düz metin bir körleştirme işlevinden geçirilerek körleştirilmiş metin elde edilir. Körleştirilmiş metin daha sonra şifrelenir. Şifrelenmiş körleştirilmiş metin ters körleştirme işlevinden geçirilerek şifrelenmiş metin elde edilebilir. Şifrelenmiş metnin şifresinin çözülmesiyle düz metin elde edilecektir. Denklem (2.6)'da bakışımsız şifrelemeyle birlikte kullanılan körleştirmenin uygulanışı gösterilmiştir.

$$\begin{aligned}
&Körleştirme_{KörleştirmeÇarpanı}(Metin)=KörleştirilmişMetin\\
&Şifreleme_{GizliAnahtar}(KörleştirilmişMetin)=ŞifrelenmişKörleştirilmişMetin\\
&TersKörleştirme_{KörleştirmeÇarpanı}(ŞifrelenmişKörleştirilmişMetin)=ŞifrelenmişMetin\\
&ŞifreÇözme_{AçıkAnahtar}(ŞifrelenmişMetin)=Metin
\end{aligned} \quad (2.6)$$

Körleştirme işlevini kullanan ile şifreleme işlevini kullananın farklı taraflar olduğu varsayılırsa, metni şifreleyen tarafın elinde körleştirme çarpanı olmadıkça metnin içeriğini görmesi olanaklı olmayacaktır.

2.3.6 Eşişlemli Şifreyazım

Grup oluşturan düz metinler uzayındaki bir işlemin karşılığı olan bir işlem grup oluşturan şifrelenmiş metinler uzayında varsa ve bu düz metinler uzayındaki herhangi bir metnin şifrelenmiş metinler uzayına eşleyen anahtarlardan bağımsız bir anahtar ile şifrelenmiş metinler uzayının bir bölümünün şifresi çözülebiliyorsa eşişlemli (homomorphic) şifreyazımdan söz edilebilir. Başka bir deyişle, eşişlemli şifreyazım şifrelenmiş metnin şifresini çözmeden üzerinde işlem yapmaktır.

$$\begin{aligned} &\text{Şifreleme}_{AnahtarA}(MetinA) = \text{ŞifrelenmişMetinA} \\ &\text{Şifreleme}_{AnahtarB}(MetinB) = \text{ŞifrelenmişMetinB} \end{aligned} \tag{2.7}$$

Denklem (2.7)'de gösterilen yolla oluşan iki ayrı şifrelenmiş metinden yola çıkılarak eşişlemli şifreyazım anlatılacaktır. Denklem (2.7)'de oluşan iki ayrı şifrelenmiş metin şifrelenmiş metin uzayında tanımlı bir $\otimes$ işleminden geçirilerek denklem (2.8)'deki gibi yeni bir şifrelenmiş metin oluşturulacaktır. Benzer şekilde denklem (2.7)'de gösterilen düz metin uzayında tanımlı iki metin aynı uzayda tanımlı bir $\oplus$ işleminden geçirilerek denklem (2.9)'deki gibi yeni bir metin oluşturulur. Yeni oluşan metin ile yeni oluşan şifrelenmiş metin arasındaki ilişkiyi şifreleme ve şifre çözme işlevleri için sağlayan bir anahtar, denklem (2.10)'da görülmektedir. Bu yolla her biri ayrı ayrı şifrelenmiş metinlerin hiçbirinin şifresi çözülmeden, yani içeriği görülmeden, bir araya getirilmeleri ve bir kerede şifrelenmiş metinlerin tamamının şifresinin çözülmesi sağlanabilir.

$$\text{ŞifrelenmişMetin} = \text{ŞifrelenmişMetinA} \otimes \text{ŞifrelenmişMetinB} \tag{2.8}$$

$$Metin = MetinA \oplus MetinB \tag{2.9}$$

$$\text{ŞifreÇözme}_{Anahtar}(\text{ŞifrelenmişMetin}) = Metin \tag{2.10}$$

Yukarıdaki denklemler boyunca kullanılan $\oplus$ işleminin tersinir olması gereklidir. Bu işlemin tersinir olmaması hâlinde son olarak elde edilen metinden ilkel metinlerin elde edilmesi olanaklı olmayacaktır.

Eşişlemli şifreyazımın sağladığı bir getiri bütünlük denetimini içermesidir. Eşişlemli şifreyazımın içerdiği tüm metinler doğru şekilde şifrelenmiş olmazsa son olarak elde edilen şifrelenmiş metin yapısı bozulacağından tüm metinleri bir arada içeren metne ulaşmak olanaksızlaşacaktır. Benzer şekilde, metinlerin eksik olması ya da şifrelenmiş metin uzayında kullanılan işlemde hata oluşması da metne ulaşmayı engelleyeceğinden bu tür hatalar uygulama sırasında kolaylıkla fark edilecektir.

2.4 Bir Oylamanın Sağlaması Gereken Koşullar

Bir elektronik oylama dizgesinin uyması gereken koşullar ülkeden ülkeye, oylamadan oylamaya değişmekle ve tartışılmakla birlikte bazı temeller aynı kalacaktır. Koşulların açıkça belirtildiği kaynaklardan biri "Internet Kuralları Enstitüsü" tarafından Amerika Birleşik Devletleri'nde yayınlanan "Ulusal Elektronik Oylama Çalıştayı Raporu"dur[4].

Raporda belirtilen on iki ögenin beşi uygulamaya yönelik sorunları kapsamaktadır.**Tablo 2.1**'de açıklanan yedi koşul dizgenin teknik yeterliliğiyle ilgili olacaktır.

Tablo 2.1 Elektronik oylamanın koşulları

Bireysellik	Sadece geçerli seçmenlerin oy kullanmasına izin verilir.
Tekillik	Her seçmenin sadece bir kez oy kullanmasına izin verilir.
Kesinlik	Dizge oyları doğru şekilde saklamalıdır.
Bütünlük	Bir oy sezilmeden silinememeli ya da değiştirilememelidir.
Denetlenebilirlik	Oylama sonucu denetlenebilmelidir.
Gürbüzlük	Oylama bağlantının geçici kesilmelerinden etkilenmemelidir.
Gizlilik	Seçmenlerin kullandıkları oylar açığa çıkmamalıdır.

2.5 Koşulların sağlanmasındaki zorluklar

Uygulamada bir elektronik oylama dizgesinin karşılaştığı sorunlar genelde alışıldık oylama dizgelerindekinden çok farklı değildir. Her oylamada en büyük sorunu oluşturan, sandık görevlilerinin ya da seçmen kartlarının hazırlanmasıyla görevli kişilerin güvenilirliği, önerilen yönteme göre elektronik oylama dizgelerinde de söz konusu olabilir. Gerçekte her oylama üç bölüme ayrılarak incelenebilir: kayıt, oy verme ve oy sayımı. Elektronik oylama dizgelerinde insan etkisinin en yüksek

olduğu aşamalar birinci ve ikinci aşamayken, sayısal etkiler ikinci ve üçüncü aşamada yüksektir.

Kayıt aşamasında bir seçmenin geçerliliği bugüne kadar ancak bir başka insan tarafından onaylanmıştır. Teknolojik olarak bunun önüne geçmek günümüzde olanaklı olsa da ancak bireysel gizliliğin yitirilmesiyle sağlanabilir. Görece pahalı olmakla birlikte, biyolojik kimlik belirleme yöntemleri yeterince başarılı sonuçlar vermektedir. Sahip olunacak bir DNA, parmak izi ya da retina kitaplığı seçmenleri tanımayı neredeyse hatasızlaştırabilir fakat bunun neden olacağı toplumsal tepkilerin de şiddetli olacağı yadsınamaz. Kaldı ki, biyolojik kitaplıkların kullanılması ve oluşturulması da kişinin doğumuna kadar gerileyen etkin bir izleme dizgesini gerektirecektir. Kısaca, aynı kişinin birden fazla oy kullanması ya da ölüler adına seçmen kartı alınması gibi eskiden beri yürürlükte olan hilelerin önüne geçecek etkin bir yöntem önermek oldukça zor görünmektedir. Bu durumda, bir elektronik oylama dizgesinden beklenen bireysellik ve tekillik kayıt aşamasının ardından incelenmelidir.

Oy verme aşamasında merkezî elektronik oylama dizgeleriyle yaygın elektronik oylama dizgeleri arasında bazı farklar görülecektir. Merkezî elektronik oylama dizgelerinde sandık görevlilerinin güvenilirliği ön plandadır. Kötü niyetli bir görevlinin seçmenleri yok yere sırada bekleterek bezdirmesi en kolay ve denetlenmesi en zor hiledir. Bunun dışında, görevlinin seçim merkezinin yetkeyle bağlantısını bozması ya da dizgenin yapısına göre oyları yetkeye teslim etmemesi olasılıkları vardır. Yaygın elektronik oylama dizgelerinde ise sorun seçmenlerin güvenilmezliğindedir. Evindeki bir konağı kullanarak oy vermeyi deneyen bir seçmenin konağın üzerinde sınırsız etkisi vardır ve bu etki hileyi olanaklı kılabilir. Dahası, bu tür dizgelerde seçmenlerin bir araya gelerek hileye girişmeleri de engellenmelidir.

Sayım aşamasında da kullanılmış geçerli oyların bir bölümünün elektronik olarak silinmesi, değiştirilmesi ya da yeni oylar oluşturulması olasılığı olacaktır.

Geneline bakıldığında, bir seçmen için elektronik oylama dizgelerinin güvensiz yanı somut olarak izleyemeyeceği bir oyun kullanılmış olması olabilir. Seçmenlerin hangi oyu kullandıklarını belgeleyen bir kağıt alması bu sorunu çözerken oy satışı tehlikesini ortaya çıkarır. Bu soruna da etkin bir çözüm bulunursa, olasılıkla, güvenilir bir dizgeye giden yol açılmış olacaktır.

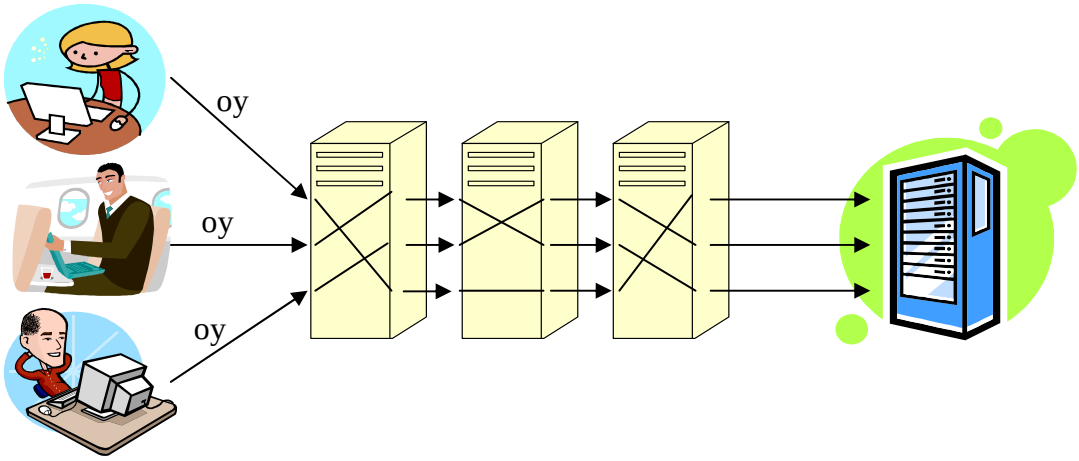
3 GEÇMİŞ ÇALIŞMALAR

Güncel elektronik oylama yöntemleri gözden geçirildiğinde üç temel yaklaşımla karşılaşılmaktadır. Bu yaklaşımlar, bunların bir arada kullanılmalarıyla oluşan yaklaşımlar ve uygulamaya yönelik düzenlemelerle birlikte önerilen dizgelerin sayısı oldukça artmaktadır. Sayının çokluğuna rağmen, üç temel yaklaşımın anlatılması konunun kavranması için yeterli görünmektedir.

3.1 Karıştırıcı Ağ Tabanlı Yaklaşım

Üç yaklaşımdan ilki karıştırıcı ağ altyapısıyla oluşturulandır. Bu yaklaşım ilk olarak Chaum'un çalışmasıyla[8] ortaya çıkmış, yıllar içinde çok sayıda değişiklikle çok sayıda örneği verilmiştir.[9-13]

İlk olarak elektronik postanın anonimleştirilmesini sağlamak için önerilen karıştırıcı ağlar bir sunucular dizisinden oluşur. Her sunucu giriş olarak bir dizi ileti alır ve bunların permütasyonunu çıkış olarak üretir. Her sunucunun çıkışı diğer bir sunucunun girişine bağlıdır.



Şekil 3.1 Örnek karıştırıcı ağ yapısı

Elektronik oylama için kullanıldığında girişler seçmenlerin oyları olacaktır. Bir gözlemcinin hangi girişin hangi çıkışa eşlendiğini bulması olanaksız olmalıdır. Aksi durumda elektronik oylama sırasında gizlilik sağlanamaz.

Elektronik oylamalarda kullanılmak üzere farklı iyileştirmelerle farklı tasarımlar önerildiyse de Chaum'un ilk önerisindeki yapı büyük ölçüde korunmuştur. Bu yapıda gönderilen metnin sırayla dolaşacağı sunucuların açık anahtarlarıyla ters sırada şifrelenmesi gerekecektir. Her sunucu kendine gelen iletinin şifresini çözerek kendinden sonraki sunucuya aktarır.

Bir karıştırıcı ağ dizgesi elektronik oylama için kullanıldığında her bir sunucunun işlemleri doğru yaptığını belgelemesi de gerekecektir. Kullanılan değişik yöntemler olsa da, örnek olarak şu yöntem verilebilir: sunucular her adımda kendilerine ulaşan iletilerin şifresini çözerken iletinin özünü de sırayla şifrelerler. Şifrelenen öz sayım aşamasında ters sırada çözülerek oyun geçerliliği denetlenir. Aksi hâlde, sunucu doğru bir şekilde şifrelenmiş sahte bir oy oluşturup farkına varılmadan bununla gerçek oyu değiştirebilir.

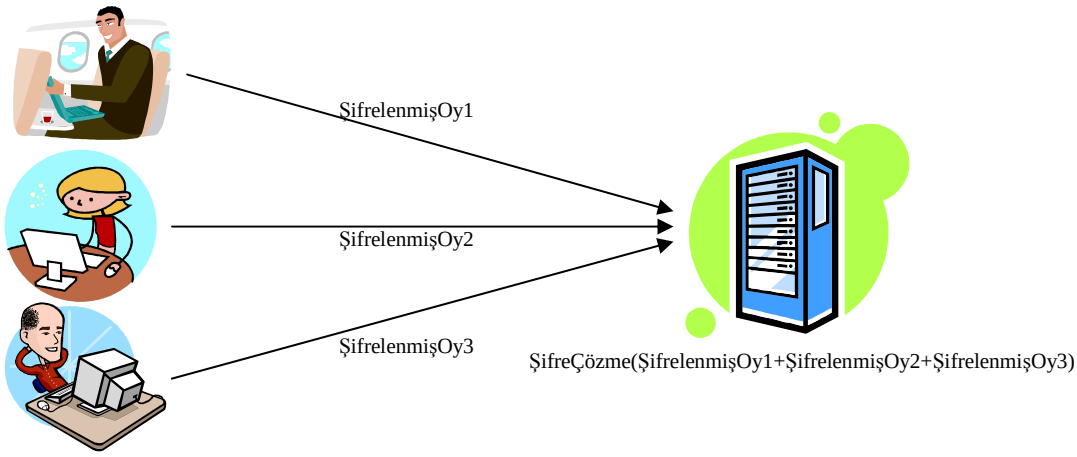
Bir karıştırıcı ağ dizgesinde permütasyonu gerçekleştiren sunuculardan birinin dürüst olması dizgenin anonimliğinin sağlanması için yeterlidir.

Bir elektronik oylama dizgesinde kullanıldığı düşünülen ayrıntısız çizilmiş bir karıştırıcı ağ yapısı **Şekil 3.1**'de görülebilir.

3.2 Eşişlem tabanlı yaklaşım

İkinci yaklaşım ilk olarak Benaloh tarafından önerilen ve daha sonra geliştirilen [7] eşişlem tabanlı yaklaşımdır. Bu yaklaşımla önerilen birçok tasarım olmuştur [15-18].

Eşişlem tabanlı yaklaşımda genelde oluşturulan; bir ya da birden çok, sıradüzenli ya da dağıtık bildirim panosunun herkese açık olarak yaratılmasıdır. Yaratılan bu panoya herkes erişiminin izin verdiği ölçüde veri yazabilecektir. Panonun yanı sıra yapıda yer alan sıradüzenli ya da dağıtık yetkili sunucular vardır. Bu sunucuların sağladıkları anahtarlarla ayrı ayrı şifrelenen metin, yani bir elektronik oylama işleyişinde oy bilgileri, diğer seçmenlerin kullandıkları oylarla bir araya geldiğinde tüm oylamanın sonucu tek seferde öğrenilecektir. Otoritelerin ya da panoların sayısı, panoların ve seçmenlerin asıllanması tasarımdan tasarıma farklılıklar göstermektedir. Basitçe gösterilen bir eşişlem tabanlı oylama dizgesi **Şekil 3.2**'de gösterilmiştir.



Şekil 3.2 Örnek eşişlem tabanlı oylama dizgesi

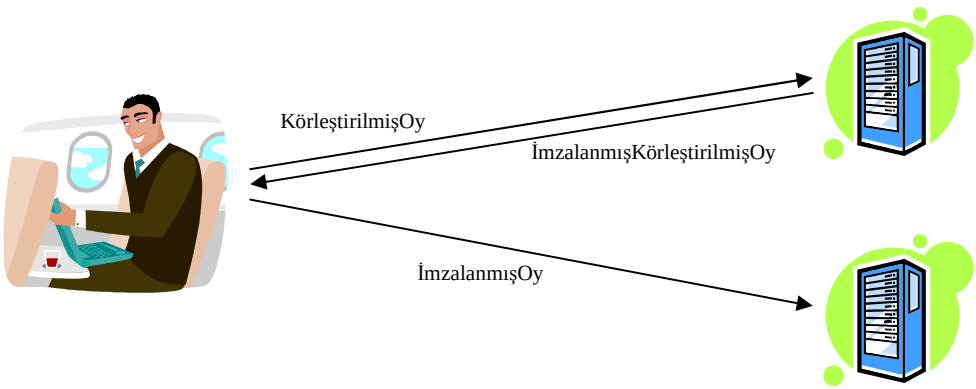
Eşişlem tabanlı yaklaşımda tek bir seçmenin hatalı oy vermesinin önüne geçmek için genelde seçmenin oyu panoya kabul edilirken oyun geçerli olduğunun belgelenmesi de istenir. Bu durumda seçmenin geçerli bir oy verdiğini belgeleyecek şifrebilimsel yöntemleri de kullanması gerekecektir[15]. Benzer şekilde, yöntem sıradüzenli sunucuları ya da panoları içeriyorsa her bir seçmen tarafından panoların her birine kaydedilen oyun aynı olduğunu belgeleyen şifrebilimsel yöntemler de kullanılmalıdır.

3.3 Körleştirme tabanlı yaklaşım

Körleştirme tabanlı yaklaşımlarda da önerilerin sayısı oldukça fazladır [19-27]. Genelde uygulanan şudur: Seçmen kullanmak istediği oyu kurallara uygun biçimde hazırladıktan sonra bunu körleştirir. Körleştirilen metin bir ya da birden çok yetkili sunucuya gönderilir. Sunucu ya da sunucular bu metni kendi gizli anahtarıyla şifrelerler. Sunucu ya da sunucular hazırladıkları şifrelenmiş körleştirilmiş metinleri tekrar seçmene gönderirler. Seçmenin bundan sonra yapması gereken körleştirme faktörünü kullanarak yetkili sunucularca şifrelenmiş metinleri elde etmek olacaktır. Seçmen kolaylıkla tamamlanan işlemlerin ardından elde ettiği imzalanmış metinlerin doğruluğunu yetkili sunucuların açık anahtarıyla elindeki şifrelenmiş metinlerin şifresini çözerek denetledikten sonra, elindeki şifrelenmiş metinleri sayımla

yetkilendirilmiş sunucuya gönderir. Sayımla yetkilendirilmiş sunucu kendisinde toplanan şifrelenmiş metinlerin şifrelerini çözer ve metinleri yayınlar.

Oyları onaylamakla yetkilendirilmiş sunucuların yerleşiminde olduğu gibi, sayımla yetkilendirilmiş sunucuların da sayısı artırılabilir. Böylece, sayım sonucunun değerlendirilmesi daha verimli olacaktır. Körleştirme tabanlı yaklaşımlarda sayımla yetkilendirilmiş sunuculardan birinin ya da birkaçının hatalı bilgi vermesini ya da oylama sonucunu değiştirmeye yönelik hareketlerini kısıtlamak üzere genelde birden çok yetkili içeren tasarımlar sunulmuştur. Yetkililerin birbirleriyle çeliştikleri, farklı sonuçlar gösterdikleri durumlarda hatanın giderilmesi ve dizgenin tutarlı çalışması için Bizans anlaşmaları[28] kullanılarak güvenilir yetkili kümeleri belirlenmektedir. Basitleştirilmiş bir körleştirme tabanlı oylama dizgesi **Şekil 3.3**'te gösterilmiştir.



Şekil 3.3 Körleştirme tabanlı örnek oylama dizgesi

4 ÖNERİLEN YÖNTEMLER

Geçmişte önerilen yaklaşımların her birinin getirileri ve götürüleri vardır. Geçmiş çalışmalarda yapılan yaklaşımların eksikleri diğer yaklaşımlarla kapatılmaya çalışılmış, bu yolla melez dizgeler elde edilmiştir. Şifrebilimsel ya da diğer yollarla var olan eksikler kapatılmaya çalışılmıştır.

Geneline bakıldığında, karıştırıcı ağ tabanlı dizgelerin eksiği, yapısı gereği bir karıştırıcı ağın verimli veri iletişimi yapamamasıdır. Söylendiği gibi, bir karıştırıcı ağda iletilen bir veri, ağın sahip olduğu her sunucuya bir kez uğrar ve her sunucuda diğer verilerle bir permütasyona sokulur ve bunun yanında bazı şifrebilimsel işlevlerden geçirilir. Elektronik oylama yapıları için özelleştirilmiş karıştırıcı ağlar ilkellerine göre oldukça verimli olsa da, yoğun katılımlı bir oylama için, örneğin ülke çapında yapılacak bir siyasî oylama için, verimlilik yeterli görünmemektedir.

Eşişlem tabanlı dizgelerde sadece iki seçenekli, örneğin “evet” ve “hayır” içeren, oylamaların yapılması olanağı vardır. İkiden çok sayıda aday içeren ya da sınırlı sayıda aday değil de, seçmen tarafından belirlenecek aday adları içeren bir oylamanın eşişlemli dizgelerle gerçekleştirilmesi olanaksız görülmektedir. Çok sayıda adayla oylama yapılmasını sağlamak için seçmenlerin oylarını ikili parçalara ayırarak her parça üzerinde ayrı ayrı eşişlemli dizgeler uygulamak ya da arka kapı içeren bazı şifreleme algoritmaları[15] kullanmak çözümler arasındadır. Gerçekte, eşişlem tabanlı şifreyazımın yapısı gereği arka kapılan barındıran yöntemler olduğu da söylenebilir. Bunların dışında, eşişlem tabanlı dizgeleri karıştırıcı ağ tabanlı dizgelerle birleştirerek elde edilen melez çözümler de seçmen tarafından aday adı yazılarak oylama yapılması için gereken aracı oluşturur. Bu çözümde önceden bilinen adaylar eşişlem tabanlı dizge aracıyla sayılırken, seçmenin yazmış olduğu önceden bilinmeyen adayları gösteren oylar diğer dizgeyle eşzamanlı çalışan karıştırıcı ağ tabanlı dizge tarafından sayılır.

Körleştirme tabanlı dizgelerin eksiklerinden biri, sayım esnasında sayımla yetkilendirilmiş sunucu ile seçmenler arasında anonim haberleşme kanalları gerektirmesidir. Sayımla yetkilendirilmiş sunucunun ağ trafiğini izleyerek –

olasılıkla– seçmenlerin ayrı ayrı verdikleri oyları belirleyebilmesi bu haberleşme kanalını zorunlu kılar. Bu sorunun üstesinden gelmek için sayımla yetkilendirilmiş sunucuların ağı izlemesini önleyecek önlemler alınması gerekir. Bu önlem sayımla yetkilendirilmiş sunucuların önüne yerleştirilecek bir karıştırıcı ağ olabilir. Karıştırıcı ağ yapısı gereği anonimliği sağlayacaktır: Bununla birlikte, körleştirme tabanlı dizgelerde sayım aşamasında yetkilendirilmiş sunuculara güvenilmesi gerekmektedir. Kıyaslandığında, diğer dizgelerde herkes tarafından sayımın denetlenmesi olanağı vardır.

Özetle, sözü edilen çalışmaların tamamı gerçek zamanda çalışan, bu yolla oylama sırasında yüksek hesap gücü gerektiren çalışmalardır. Bu çalışmada birbirine benzer iki ayrı çevrimdışı elektronik oylama dizgesi önerisi sunulacaktır. Önerilerin olumlu ve olumsuz yönleri ise güvenliğin tartışıldığı bölümde ayrıntılarıyla ele alınacaktır.

Sunulan önerilerden birincisinde oy verme işleminin her seçmence sadece bir kere gerçekleştirilebileceği düşünülmüştür. Aksi olanaklıysa da, önerilen dizgenin işleyişini alışıldık elle sayım dizgelerine benzetmek amacıyla oylama sonuçlarının oylama süresinin dolmasının ardından açıklanacağı varsayılmıştır.

İkinci öneride birinci öneridekinin aksine, bir seçmen oylama süresi dolana kadar oyunu değiştirebilecektir. Bu, oy satılması olasılığını azaltmak için önerilmiştir. İlkine benzer şekilde, bu dizgede de oylama sonuçlarının oylama süresinin dolmasından sonra açıklanacağı varsayılmıştır.

Dikkat çekici bir nokta, seçmenlerin kullandıkları oyların gerçek zamanda açıklanması ile oylama sonunda açıklanmasının oylamanın işleyişine getireceği farktır. Oylar gerçek zamanda açıklanacak olursa, diğer seçmenlerin yönelimine göre seçmenlerin tepkisi değişebilir. Bu özellik, ilk bakışta, seçmenlerin karar vermesine yardım edeceği düşünülerek daha dürüst oylama sonuçları sağlayacakmış gibi görünse de bunun toplumsal tartışmalarla karara bağlanması gereken bir konu olduğu düşünüldüğünden bu çalışma içinde yorum yapılmamıştır.

4.1 Tanımlar

Her iki öneride de kullanılan ögeler, dolayısıyla bunların tanımları benzerdir. Ögelerin tanımlanmalarıyla öneriler daha yalın anlatılabilir.

4.1.1 Taraflar

Yöntemler üç taraf içerir: Yetke, Seçmen ve Sayman.

Yetke, geçerli seçmenlerin kayıtlarını tutan ve seçmenin geçerli oy kullandığını belgeleyen taraftır. Oylama öncesinde seçmenler yetkeye seçmen olduklarını kanıtlarlar ve yetkeyle gerekli anahtarların alışverişini yaparlar.

Sayman, yetkenin geçerli olduğunu belgelemiş olduğu oyları seçmenlerden bağımsızlaştırarak saklar. Sayman yöntemin güvenilirliğini artırmak amacıyla birden çok sayıda bağımsız konaktan oluşmuş olarak da tasarlanabilir. Anlatımda basitliği sağlamak amacıyla öncelikle sayman tek konaktan oluşuyormuş gibi düşünülecek, çok konaktan oluşan saymanın getirileri güvenliğin sorgulandığı bölümde açıklanacaktır.

Seçmen, yetke ile kayıt sırasında yapmış olduğu anahtar alışverişi ile korunan bir oturum başlatarak yetkeye ilişkin bir etmen çalıştırır. Bu etmenin ve seçmenin birlikte çalışmasıyla saymana ilişkin bir başka etmen seçmenin bilgisayarına taşınır. Gerekli tüm hesaplamalar seçmenin bilgisayarında gerçekleştikten sonra etmenler sonlandırılır, saymana ilişkin etmen seçmenin oyunu saymana bildirir.

4.1.2 Anahtarlar

Yöntemler temelde üç bakışımsız anahtar çifti ve bir bakışımlı anahtar ile işlemektedir: yetkeye ilişkin anahtar çifti, her bir seçmene ilişkin anahtar çifti, saymana ilişkin anahtar çifti ve bir oturum anahtarı.

Yetkeye ilişkin anahtar çifti yetke tarafından kayıt aşamasından önce oluşturulur. Kayıt aşamasında geçerli her seçmene yetkenin açık anahtarı teslim edilir. Yetkenin gizli anahtarı seçmenlerin kullandıkları oyların geçerliliklerini kanıtlamak ve yetke ile seçmen arasında güvenli iletişimi sağlamak için kullanılacaktır.

Saymana ilişkin anahtar çifti sayman tarafından oluşturulacak ve oylama başlamadan önce saymanın açık anahtarı yetkeye teslim edilecektir. Bu anahtar çifti saymana ilişkin etmenlerin ve seçmenlerin oylarının güvenli taşınması için kullanılacaktır.

Seçmene ilişkin anahtar çifti kayıt aşamasından önce yaratılacak ve kayıt aşamasında her seçmen açık anahtarını yetkeye teslim edecektir. Bu anahtar çifti yetkenin seçmeni asıllamasında kullanılacaktır.

Oturum anahtarı oylama öncesinde yetke tarafından her bir seçmen için oluşturulacaktır. Bu anahtar yetkeye ilişkin etmenlerin güvenli taşınması için kullanılacaktır.

4.1.3 Etmenler

Yöntemler iki etmen barındırmaktadır: kayıt defteri (kısaca defter) ve oy pusulası (kısaca pusula).

Defter, yetkenin uzantısı olarak seçmenin oy kullandığı konağa yerleşecek, seçmenin oyunun geçerliliğini belgeleyecek ve saymanın uzantısı olan pusulaya teslim edecektir. Defter, seçmenin oyunu geçerli kılacak işlemlerin ardından sonlandırılacaktır. Kısaca, defter etmeninin alışıldık oylamalardaki kayıt defterinin görevini üstlendiği söylenebilir.

Pusula, saymanın bir uzantısı olarak seçmenin oy kullandığı konağa yerleşecek, seçmenin oyunu defterden gizleyerek deftere imzalatacaktır. Daha sonra bu oyu saymana göndererek sonlanacaktır. Özetle, pusula etmeni alışıldık oylama dizgelerindeki oy pusulasının işlevini üstlenecektir.

4.2 Birinci Yöntem

Önerilecek yöntemle bilinen körleştirme tabanlı yaklaşımı etmenlere uyarlamayı deneyen bir merkezî çevrimdışı elektronik oylama dizgesi gerçekleştirilebilir. Yöntem üç taraf içerir. Taraflardan ikisinin uzantısı olacak etmenler tasarlanmıştır. Bu etmenler üçüncü tarafa ilişkin bilgisayarda çalışarak hesaplamaları yapacak ve oy verme işlemini tamamlayacaklardır. Önerilen yöntemin uygulanabileceği bir dizgenin işleyişi anlatılırken uygulamada karşılaşılabilecek birçok aykırılık dizgenin güvenliğinin incelendiği bölüme bırakılarak doğrusal bir anlatım seçilmiştir. Anlatım sırasında yer yer belirtilen şekillerin anlaşılmasında yararlı olacak **Tablo 4.1** aşağıda verilmiştir.

Tablo 4.1 Şekillere ilişkin açıklamalar

Kesik kenarlı dikdörtgen	Oy kullanma işlemi sırasında kullanılan konak. Konağı o sırada kullanan seçmene ilişkin im dikdörtgenin sağ alt köşesinde belirtilir.
Sunucu	Yetkeyi ya da saymanı belirtir. Yetke bir terâzi imi ile, siyasî partilerin koalisyonuyla oluştuğu varsayılan sayman ise koalisyona katılan siyasî partilerin imleri ile belirtilir.
Anahtar	Şifreyazımsal anahtarı belirtir. Anahtarın sahibi sol alt köşesine eklenmiş im ile belirtilir.
Defter	Defter etmenini belirtir. Etmenin sahibi sol alt köşesine eklenmiş im ile belirtilir.
Oy pusulası	Pusula etmenini belirtir.
Eğik ok	Bir konakta bir yazılım nesnesinin oluşturulduğunu ya da bir konağa başka bir kaynaktan bir yazılım nesnesinin eklendiğini gösterir. Yazılım nesnesi konakta oluşturuluyorsa ok konaktan yazılım nesnesine yöneliktir. Konağa bir yazılım nesnesi ekleniyorsa ok yazılım nesnesinden konağa yöneliktir.
Kalın ok	Zamanda bir akışı gösterir. Zamandizinsel olarak ilk gerçekleştirilen olayı gösteren şekilden daha sonra gerçekleştirilen olayı gösteren şekle yönelmiştir.
Ok	Seçmen, etmenler, konaklar, sunucular arasındaki iletişimi ya da etmenlerin devinimini gösterir. Eğer bir iletişimi gösteriyorsa, iletiler okun üstünde belirtilir.

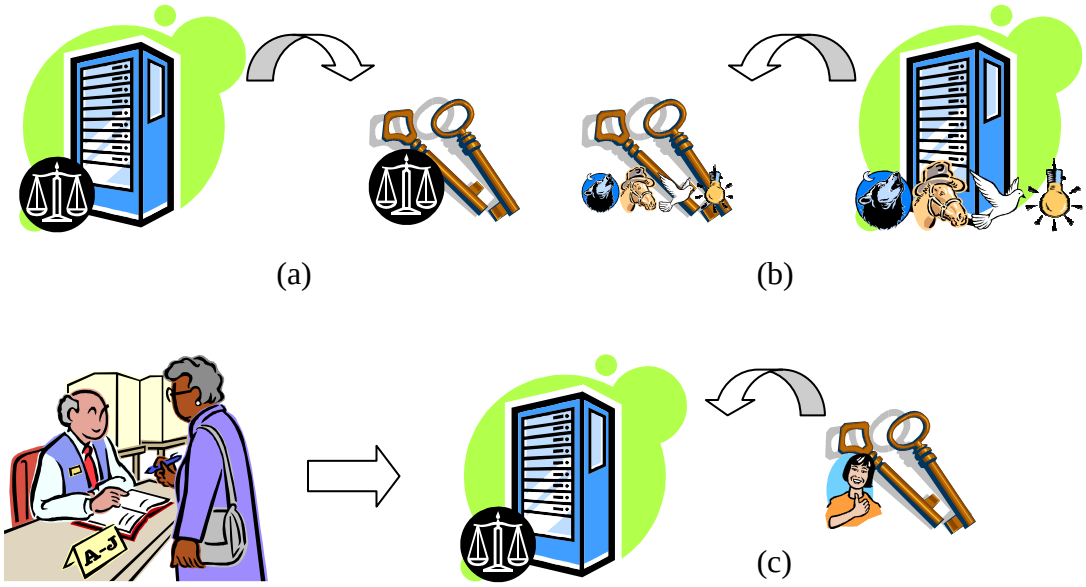
4.2.1 Dizgenin İşleyişi

Her oylamanın üç aşamadan oluştuğu düşünülebilir. Kayıt aşaması, oy verme aşaması ve sayım aşaması. Bu üç aşamanın güvenlikleri ayrı ayrı sağlanmalıdır.

Herhangi bir adımdaki güvenlik açığının diğer aşamaları da etkileyeceği açıkça bellidir.

Kayıt aşamasından önce sayman ve yetke anahtar çiftlerini hazırlarlar. Bu adım **Şekil 4.1a**'da ve **Şekil 4.1b**'de görülebilir. Sayman kendine ilişkin açık anahtarı kayıt aşamasında seçmenlere dağıtılmak üzere yetkeye verir.

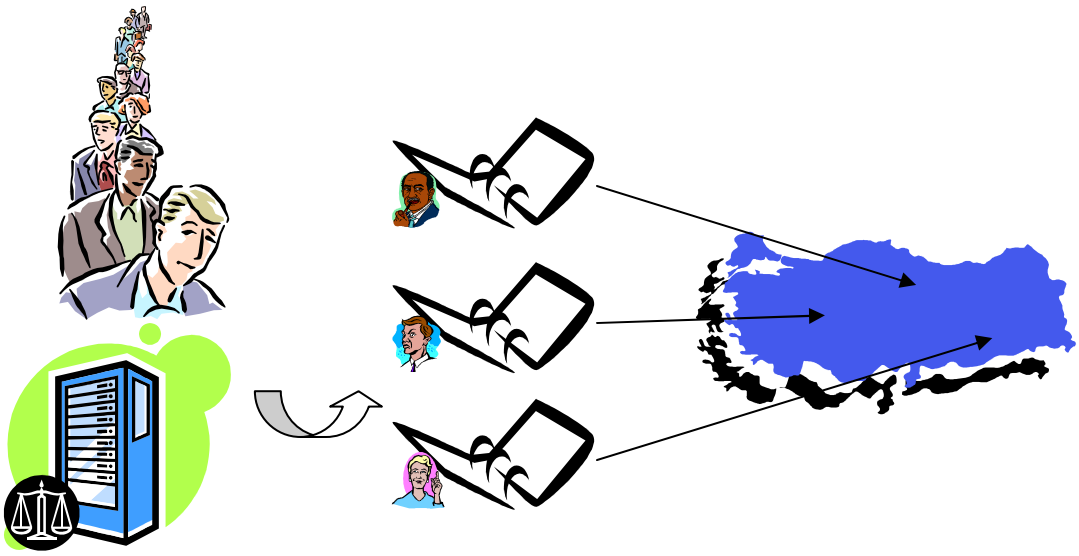
Kayıt aşamasında yetkeye başvuran geçerli seçmenlerin açık anahtarları kabul edilir ve saklanır. Bu adım **Şekil 4.1c**'de görülebilir. Her bir seçmene yetkenin açık anahtarı ve oylamayı başlatacak olan veriler ve/veya yazılım parçaları verilir. Kayıt sırasında seçmenlere verilecek verilerin hangi biçemde taşınacağı tartışmaya açık olmakla birlikte, bunun için önereceğimiz biçem herhangi bir veri saklayıcıda tutulabilir kabul edilmiştir. Bu veri saklayıcı bellek çubuğu ya da harici disk olabileceği gibi, daha güvenli olan ve görece fiyatı ucuzlamış olan akıllı kartlar da olabilir.



Şekil 4.1 Kayıt Öncesinin ve Kayıt Aşamasının Görsel Anlatımı

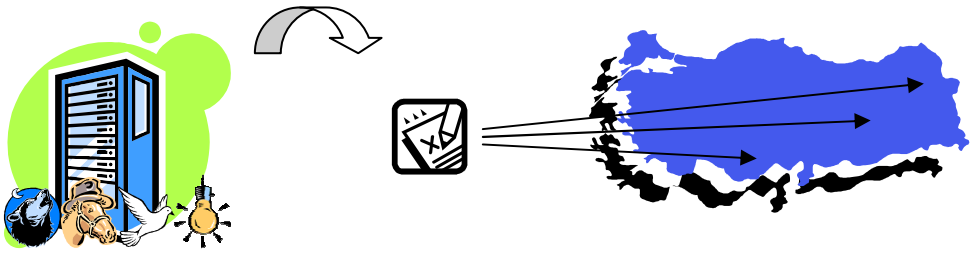
Kayıt aşamasından sonra oy verme aşamasından önce, seçmenler için etmenler hazırlanmalıdır. Her seçmenin kendine özgü defter etmeni yetke tarafından hazırlanır. Çevrimdışı yürüyen bu aşama **Şekil 4.2**'de görülebilir. Bu aşamada her bir defter etmeninin içine yetkenin gizli anahtarı ve saymanın açık anahtarı yerleştirilir.

Bu aşamayı gerçek zamanda yapmamak, oluşturulan defter etmenlerinin yerel sunuculara dağıtılması için yeterli zaman sağlar. Böylece oylamanın sıradüzenli bir şekilde yapılması sağlanabilir ve ağ üzerinde yoğun trafik olan sıcak noktaların oluşması engellenir.



Şekil 4.2 Defter etmenlerinin hazırlanışı

Oy pusulası etmeni tüm seçmenler için aynıdır ve Sayman tarafından hazırlanır. Oy pusulasının hazırlanışı **Şekil 4.3**'de gösterilmiştir.

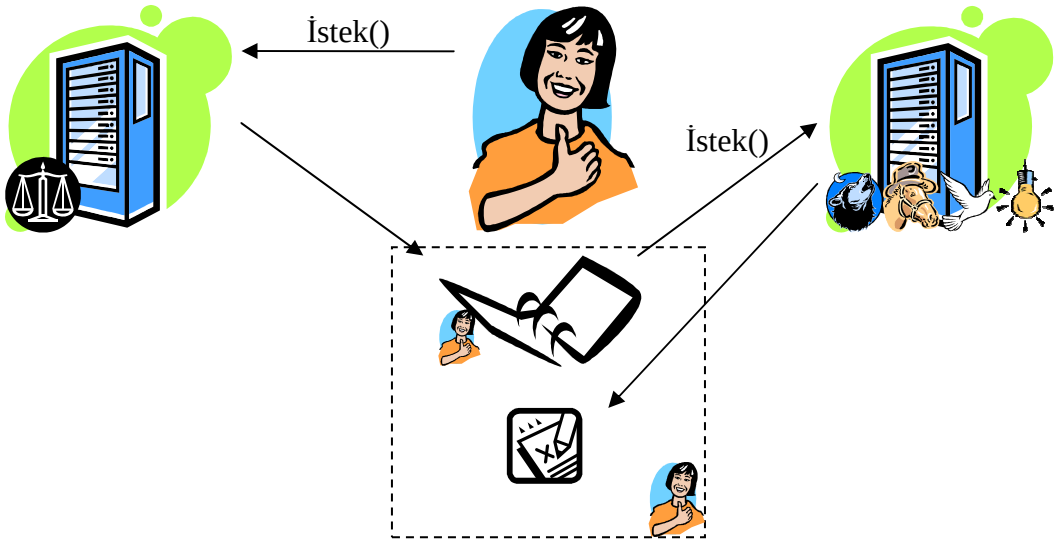


Şekil 4.3 Pusula etmeninin hazırlanışı

Oy verme aşamasında seçmenlerin tamamının kaydının yapılmış olduğu varsayılacaktır. Hatalı bir kayıt bir önceki aşamada yapılmışsa bu aşamada hatalı kaydedilen seçmenin oyunun geçersiz sayılacağı gözden kaçmamalıdır. Oy verme

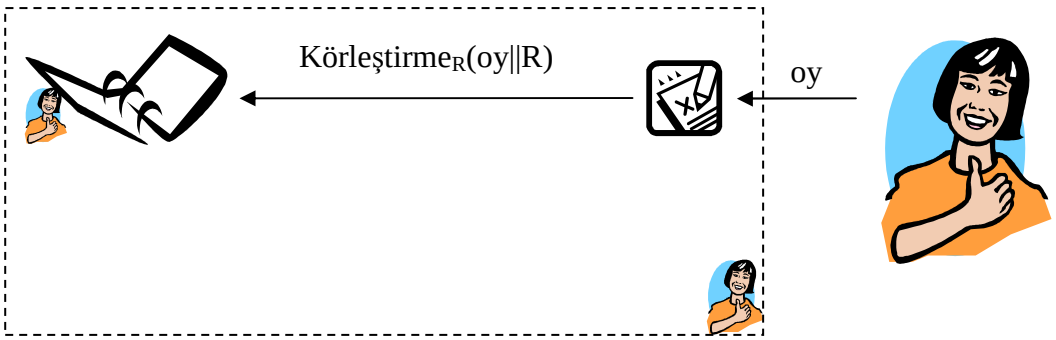
işlemi sırasında her bir seçmenin oy verip vermediği izlenmeli, bununla birlikte, seçmenin kullandığı oy sayım aşamasına kadar ortaya çıkmamalıdır. Oylama sırasında seçmenler kayıt aşamasında edindikleri şifrebilimsel anahtarlar ve gerekiyorsa biçemin içerdiği diğer verileri kullanacaklardır.

Seçmen oy vermek için kayıt numarası ile yetkeye başvurarak oy verme işlemini başlatır. Seçmenin gönderdiği ileti iki parçadan oluşur. İlk parçada yetkenin açık anahtarı ile şifrelenmiş biçimde seçmenin kayıt numarası bulunur. İkinci parçada da yine seçmenin kayıt numarası bu kez kendine ilişkin gizli anahtarla şifrelenmiştir. Burada sözü edilen kayıt numarası seçmenleri birbirinden ayırmaya yarayacak herhangi bir sayı olabilir, örneğin kimlik numarası kullanılabilir. Yetkenin seçmene gönderdiği paketin içindeki defter etmeni oturum anahtarı ile şifrelenmiştir. Oturum anahtarı da aynı paketin içinde seçmenin açık anahtarı ile şifrelenmiş olarak bulunacaktır. Seçmen aldığı paketin içinden önce oturum anahtarını alıp şifresini çözecek, sonra da oturum anahtarıyla etmenin şifresini çözecektir. Şifresi çözüldükten sonra etmen seçmenin bilgisayarında çalışır. Defter etmeni çalıştığında saymanın imzalamış olduğu pusula etmenini saymandan ister ve alır. Pusula etmeninin imzasını denetlendikten sonra çalıştırır. Etmenlerin edinilmesi **Şekil 4.4**'da gösterilmiştir.



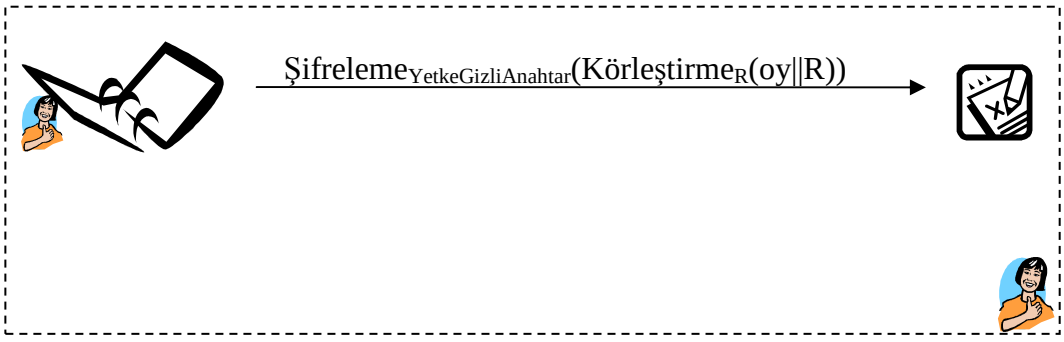
Şekil 4.4 Oy verme aşamasının başlangıcı, etmenleri elde etme.

Pusula etmeni çalışarak seçmene oyunu sorar ve **Şekil 4.5**'da gösterildiği gibi elde ettiği oyu bir rastgele sayıyla bitiştirdikten sonra körleştirerek şifrelemesi için defter etmenine gönderir.

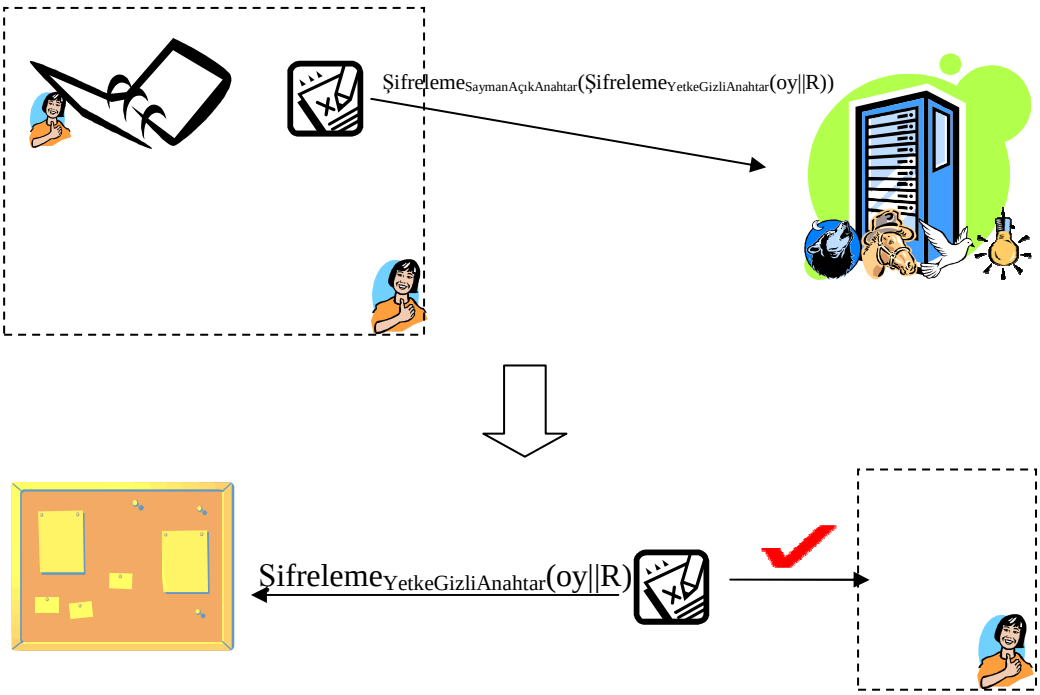


Şekil 4.5 Oyun pusula etmenine, daha sonra defter etmenine bildirilmesi

Defter etmeni pusuladan gelen iletiyi **Şekil 4.6**'deki gibi yetkenin gizli anahtarıyla şifreler. Şifrelenen ileti pusula etmeni tarafından ters körleştirme işlevinden geçirildiğinde elde edilen sayı oyun şifrelenmiş biçimidir.

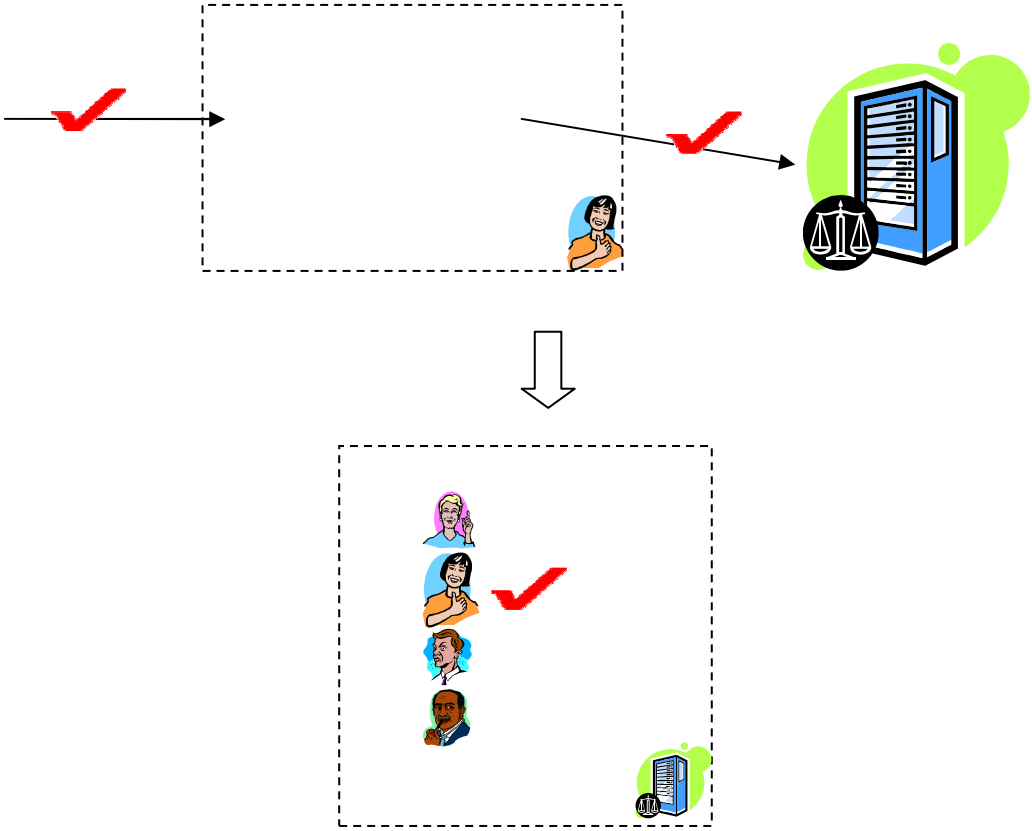


Şekil 4.6 Defter etmeninin körleştirilmiş oyu imzalaması



Şekil 4.7 Pusula etmeninin oyu sayım havuzuna iletmesi

Bundan sonra pusula etmeni oyu saymana göndererek kendini sonlandırır. **Şekil 4.7**'de gösterildiği gibi sayman oyu sakladıktan sonra seçmen oy kullandığını onaylayacak bir iletiyi **Şekil 4.8**'deki gibi yetkeye göndererek sonlanır. Seçmenin oy verdiğini onaylayan iletinin yetkeye ulaşmasıyla seçmen oy vermiş olarak işaretlenir. Seçmenin işaretlenmesiyle oy verme işlemi de sonlanmış olur.



Şekil 4.8 Defter etmeninin seçmenin oy kullandığını bildirmesi

Sayım aşamasında seçmenlerin oy verme aşamasını tamamlamış olması gerekmektedir. Eğer oy verme aşamasında oy vermemiş bir seçmen varsa, bu kişinin sayım aşamasına geçildikten sonra oy vermesinin olanaklı olmadığı gözden kaçmamalıdır. Sayım aşaması bir kere başladıktan sonra dileyen herkesin oy sayımının doğruluğunu denetleyebilmesi gerekir. Böylece, güvenilir bir elektronik oylama dizgesinin koşullarından biri daha sağlanmış olur. Oy sayımının herkesçe denetlenebilir olması, olasılıkla, toplumsal güven yaratmakta da faydalı olacaktır.

Çevrimdışı yürütülecek olan sayım aşaması oylama süresinin bitiminden sonra başlatılır. Sayman gizli anahtarıyla sakladığı oyların şifresini çözer. Daha sonra bu oyların şifresini yetkenin açık anahtarıyla da çözerek sayımı tamamlar.

Yöntemin içerdiği adımlar aşağıda özetlenmiştir. Her bir adımın güvenliği ile ilgili irdeleme ayrıt 4.2.2.1'de verilmiştir. Oy verme aşamasını gösteren UML **Şekil 4.9**'da verilmiştir.

i. Gerekli anahtarlar ve etmenler oluşturulur. Anahtar dağıtımı tamamlanır.

ii. Seçmen oy verme işlemini başlatmak üzere yetkeye *"$Şifreleme_{YetkeAçıkAnahtar}(KimlikNo)||Şifreleme_{SeçmenGizliAnahtar}(KimlikNo)$"* iletisini gönderir. İki dikey paralel çizgiden oluşan im, sağındaki ve solundaki iletilerin bitiştirildiğini göstermektedir.

iii. Yetke iletinin ilk parçasını okuduktan sonra seçmene ilişkin açık anahtarla ikinci parçayı açmayı dener. Eğer iletinin iki parçası birbirine denkse kayıtlı seçmenler arasında seçmeni arar. Seçmen kayıtlı değilse işlem iptal edilecektir. Seçmen oy kullanan seçmenler arasında aranır. Henüz oy kullanmadığı belirlenirse oy kullanma işlemi uygun şekilde başlatılır. *"$Şifreleme_{SeçmenAçıkAnahtar}(OturumAnahtarı)||Şifreleme_{OturumAnahtarı}(Defter)$"* iletisi seçmene gönderilir. Seçmen oy kullanmışsa işlem sonlandırılır.

iv. Seçmen gelen iletinin şifresini uygun biçimde çözerek defter etmenini çalıştırır. Defter etmeni saymandan pusula etmenini ister. Pusula etmenini saymanca imzalanmış olarak alan defter etmeni pusula etmenini etkinleştirir.

v. Pusula etmeni seçmenin kendisine ilettiği oyu bir rastgele sayıyla birleştirdikten sonra körleştirir. *"$Körleştirme_{KörleştirmeÇarpanı}(Oy||RastgeleSayı)$"* iletisini defter etmenine gönderir.

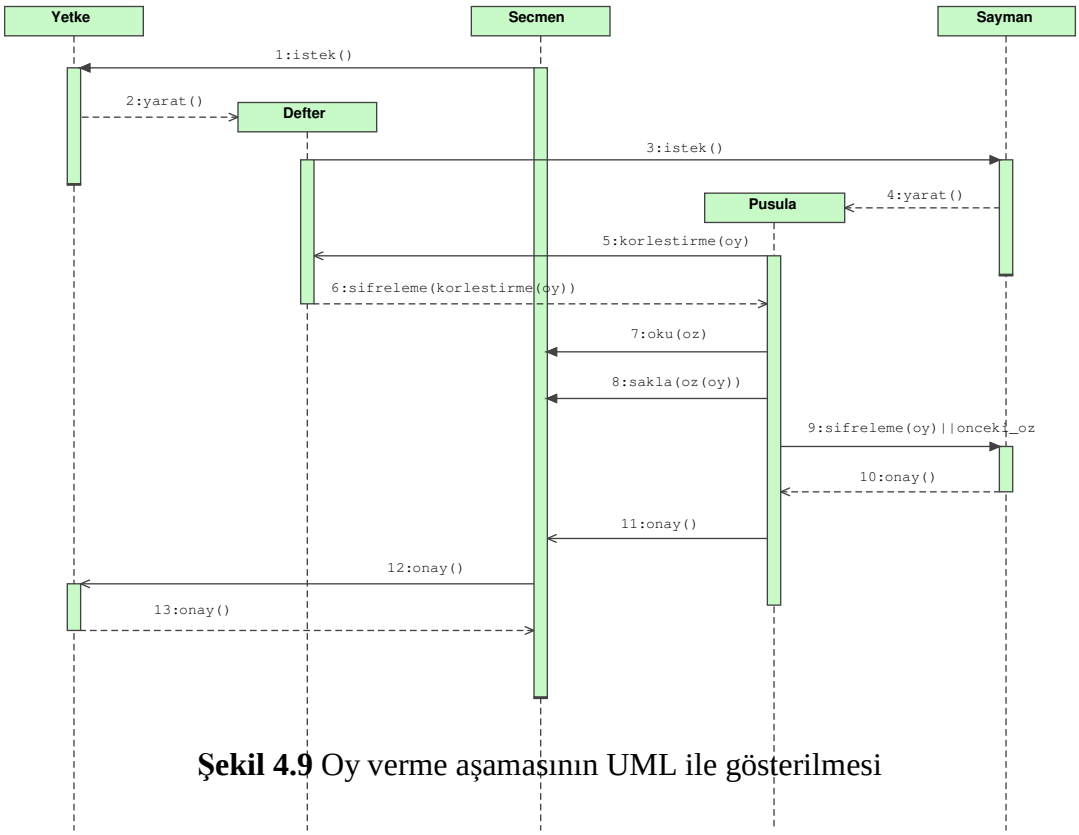
vi. Defter körleştirilmiş oyu yetkenin gizli anahtarıyla şifreler. *"$Şifreleme_{YetkeGizliAnahtar}(Körleştirme_{KörleştirmeÇarpanı}(Oy||RastgeleSayı))$"* iletisini pusulaya gönderdikten sonra sonlanır.

vii. Pusula iletiyi ters körleştirme işlevinden geçirerek *"$Şifreleme_{YetkeGizliAnahtar}(Oy||RastgeleSayı)$"* sayısını elde eder. Pusula bu sayıyı saymanın açık anahtarıyla şifreler. *"$Şifreleme_{SaymanAçıkAnahtar}(Şifreleme_{YetkeGizliAnahtar}(Oy||RastgeleSayı))$"* iletisini saymana gönderip kendini sonlandırır.

viii. Seçmen iki parçadan oluşan bir onay iletisi oluşturur. Oluşturduğu *"$Şifreleme_{YetkeAçıkAnahtar}(KimlikNo)||Şifreleme_{SeçmenGizliAnahtar}(Onay)$"* iletisini yetkeye gönderir.

ix. Yetke uygun şekilde şifresini çözdüğü iletinin anlamlı olması durumunda seçmeni oy kullanmış olarak imler.

x. Sayman saklanan oyların şifresini çözerek sayımı tamamlar.



Şekil 4.9 Oy verme aşamasının UML ile gösterilmesi

4.2.2 Güvenlikle ilgili irdelemeler

Oy verme aşamasının her bir adımının güvenliğiyle ilgili tartışmanın ardından, dizgenin güvenliği bir bütün olarak incelenecektir.

4.2.2.1 Oy verme aşamasının güvenliği

i. Anahtar dağıtımının güvenli tamamlandığı varsayılmaktadır.

ii. Gönderilen ileti hizmet engelleme saldırılarından (Denial of Service, DoS) yetkenin korunması amacıyla iki parçalıdır. İletinin ikinci parçası seçmen dışında biri tarafından oluşturulamayacağı için yetkenin yanıtladığı tüm iletiler anlamlı olacaktır. İletinin kötü emelli biri tarafından saklanıp yetkeye tekrar gönderilmesi yoluyla yetkenin hizmet vermesini engellemek olanaklı

olabilir. Bu nedenle yetke iletiler anlamlı da olsa seçmenlerin başvurularını süzerek sadece gerekli olduğunda yanıtlamalıdır.

iii. İkinci adımda belirtilenlere ek olarak, bu adımda seçmene iletilen etmen bir oturum anahtarıyla, oturum anahtarı da seçmenin açık anahtarıyla şifrelenmiştir. O hâlde, yetkenin gönderdiği etmeni görebilecek tek kişi seçmendir. Defter etmeninin iletimi sırasında ortaya çıkacak hatalı ikililer dolayısıyla seçmenin etmeni tekrar istemesi söz konusu olabilir. Seçmene ilişkin etmen daha önce gönderilmişse, bir kere daha gönderilmesi engellenebilir. Bu durumda, etmenin düzgün taşındığından emin olunması için seçmenden yüklediği etmenin sağlamasını yetkeye göndermesi istenebilir.

iv. Pusula etmeninin imzalanmış olması iletişime etki etme olasılığı olan birinin doğru çalışmayan ya da hileli bir pusula etmenini seçmene göndermesini engellemektedir.

v. Her oyu bir diğerinden ayıran rastgele sayılar oylara eşlenmiştir. Rastgele sayıların oldukça geniş bir kümeden seçildiği, yani seçilen rastgele sayıların çakışmadığı varsayılmıştır. Körleştirilmiş oyu körleştirme çarpanını bilmeden görmek olanaklı değildir.

vi. Körleştirilmiş oyun yetkenin gizli anahtarıyla şifrelenmesi, körleştirilmiş oyun yetke tarafından imzalanması olarak düşünülebilir. Yetkenin gizli anahtarı etmen içinde taşınsa da kötü emelli biri yetkili kişilerce denetlenen bir merkezdeki konağa etki etmek için yeterli zamanı bulamayacaktır.

vii. Körleştirildikten sonra imzalanan oy ters körleştirme işlevinden geçirilidiğinde elde edilen, imzalanmış oydur. Körleştirme, uygulanan işlemleri etkilememiş, sadece oyun okunmasını engellemiştir. İmzalanmış oyun saymanın açık anahtarıyla şifrelenmesi sayman dışında birinin oyu okumasını engeller.

viii. Hizmet engelleme saldırılarının engellenmesi için ikinci adımdakine benzer bir yolla ileti oluşturulmuştur.

ix. Bu adımda güvenlikle ilgili bir açıklama gerekmemektedir.

x. Bu adımda güvenlikle ilgili bir açıklama gerekmemektedir.

4.2.2.2 Dizgenin güvenliği

Dizgenin bireyselliği daha önce de değinildiği gibi, ancak kayıt aşamasından sonra incelenebilir. Dizgenin bireyselliğini sağlayan temel, defter etmeninin sadece seçmende var olan gizli anahtarla şifresi çözülebilecek bir yolla seçmene gönderilmesiyle sağlanır. Bireyselliğin sağlanmasındaki bir başka sorun seçmenin kendine ilişkin anahtarı kaybetmesi ya da bir başkasına vermesiyle ortaya çıkabilir. Ne yazık ki, seçmenin bireysel olarak anahtarını saklama yükümlülüğünde olduğunu düşünmek dışında bir çözüm biyolojik temellere dayanan asıllama yöntemlerine başvurulmadıkça görünmemektedir.

Dizgenin tekilliği, yani kaydolmuş her bir seçmenin sadece tek bir kere oy kullanması, yetke tarafında geliştirilen yaklaşımlarla çözülecektir. Yetkenin basitçe iki seçeneği vardır: defter etmenini göndermesiyle seçmenin oy kullandığını varsayması ya da seçmenin onayı ile seçmenin oy kullandığını varsayması. İkinci seçenek defter etmeninin taşınması sırasında ortaya çıkacak sorunlara karşı etkili görünmekle birlikte, kötü niyetli bir seçmenin henüz oy gönderilmemişken ikinci kere etmeni istemesiyle tekilliği bozacak bir açık yaratmaktadır. Bunun düzeltilmesi için yetke tarafında defter etmeni isteklerinin süzülmesi ve uygun şartlar altında defter etmeninin gönderilmesi sağlanabilir. Böylece olumlu ya da olumsuz bir yanıt alınmadıkça ikinci etmenin gönderilmesi engellenerek daha güvenilir görünen ikinci seçenek kullanılır.

Dizgenin kesinliğini sağlayan temel oyların ancak ve ancak doğru biçimde oluşturulduklarında anlamlı olarak sayılabilmeleridir. Gerçekten var olmayan bir rastgele oy oluşturulması denenirse, sayım aşamasında dizge için anlamsız bir veri olacağı için bu oy önemsenmeyecektir. Oluşturulan bir oyun saklanmasının ardından üzerinde yapılacak yöntemli bir değişiklikle başka bir oya dönüştürülmesi olanağı şifrebilimsel ilkeler sayesinde yoktur.

Dizgenin bütünlüğü iki ayrı yolla sağlanabilir. Birincisi, bir oyun sezilmeden silinmesini engeller. Yetke tarafından onaylanmış oyların sayısı ile sayman tarafından açıklanan oyların sayısı birbirini tutmalıdır. İkincisi, bir oyun hem silinmesini, hem de değiştirilmesini engeller. Değinildiği gibi, seçmenler kullandıkları oyları saymana göndermeden önce sadece oy kullandıkları anda geçerli olup sonradan yitirilen bir fiş ile denetleyebilmektedirler.

Dizgenin sayımı açık yapılacağından her aşamasında denetlenebilirliği sağlanmıştır.

Dizge etmen tabanlı olduğundan bağlantı sorunlarından en az etkilenecek yapıdadır. Etmenlerin düzgün taşınmaması olasılığı da etmenlerin taşınmalarının ardından bütünlük denetiminden geçmeleriyle önlenmiştir. Buna rağmen ortaya çıkacak sıradışı bir bağlantı sorununda merkezî konaklarda oy kullanılmış olmasından yararlanılabilir. Konaklarda kayıtlı olan ve henüz sunuculara gönderilmemiş oylar yetkililerce denetlenerek elle taşınabilir.

Seçmenlerin kullandıkları oyların açığa çıkmaması, yani gizlilik, her seçmen tarafından yaratılan ve körleştirme için de kullanılan rastgele sayıya bağlıdır. Her bir seçmen kendine ilişkin oyu kendi yarattığı bir rastgele sayıyla tanıyabilir. Bu sayı sadece oy verme işlemi sırasında kullanıldığından ve bu işlem sırasında rastgele sayının yetkeye taşınması olasılığı olmadığından dizgenin gizliliği sağladığı görülür.

Yukarıdaki paragraflarda açıklandığı gibi bir elektronik oylama dizgesinin sağlaması gereken koşulları sağlasa da dizgenin uygulanması sırasında karşılaşılabilecek olası sorunların bir dökümünü çıkarmak yararlı olacaktır.

Dizgenin uygulanmasında karşı karşıya kalınacak sorunların ilki, daha önce de söz edildiği gibi kayıt aşamasında ve oy verme işlemi sırasında biyolojik temelli asıllamanın getirdiği zorluktur. Biyolojik temelli asıllama kullanılmadıkça kayıt aşamasında geçerli seçmenlerin kaydedildiğinden emin olmak güçtür. Oy verme işlemi sırasında da kayıt aşamasındakine benzer şekilde seçmenlerin biyolojik temelli asıllama yöntemleri uygulanmadıkça asıllanmalarında zorluklar çıkmaktadır.

Seçmenlerin sahip oldukları konaklarda ya da merkezî konaklarda oy kullandığı düşünülebilir. Merkezî ve görevlilerce denetlenen konaklarda oy kullanılması sırasında asıllamanın güvenliği bir nebze artmış olacaktır. Seçmenlerin kendilerine ilişkin konaklarda oy kullandığı düşünüldüğünde asıllamayı denetlemek olanaklı değildir. Bu aşamada sadece seçmenlerin kendilerinde bulunan anahtarı yeterince koruduklarına güvenebiliriz. Önerdiğimiz yöntemde seçmene ilişkin gizli anahtarın güvenliği dizgenin güvenliğine değil, ancak seçmenin oy hakkının güvenliğine eşdeğerdir. Her seçmenin kendi anahtarının güvenliğinden sorumlu tutulduğu düşünüldüğünde, bu anahtarın güvenliğinin dizgenin güvenliğini etkilemeyecek yolla tasarlanmış olduğu söylenebilir.

Oy verme aşamasında da iki sorunla karşılaşılır. Birincisi oy satılması tehlikesidir. Bir seçmen kendine ilişkin bir konağı kullanarak oy verme işlemini gerçekleştiriyorsa kendisini izleyen biri seçmenin hangi seçimi yaptığını görebilir. Bu da kolaylıkla oy satılmasına neden olabilir. Bunu engellemek için en iyi yol, bu dizge dahilinde seçmenlerin görevlilerce denetlenen merkezî konaklarda kapalı odacıklarda oy kullanmalarını istemektir.

Oy verme aşamasında karşılaşılan ikinci tehlike yine seçmenlerin bağımsız konaklarda oy kullanması durumunda karşılaşılacak olan zorluklardan biridir. Etmen tabanlı yöntemin önerilmesi, temelde, etmenlerin güvenli bir şekilde devinebilecekleri altyapıya sahip bir ortamı gerektirecektir. Bu ortamı sağladığını ileri süren altyapı seçenekleri varsa da denetlemeye kapalı bir konağın güvenliğinden haklı olarak şüphe edilebilir. Etmenlerin güvenliğiyle ilgili en ciddi tehlike, yetkeye ilişkin gizli anahtarı beraberinde taşıyan defter etmeninden bu anahtarın alınmasıdır. Bu anahtarın ele geçmesi ile sahte oylar yaratılabilir. Her ne kadar sahte oy eklendiği dizge tarafından fark edilse de, hangi oyların eklendiğini fark etmek olanaklı olmayacaktır. Bu sorunun çözümü de denetlenen konaklarda oy kullanmaktır. Böylece seçmenlerin konaklara etki etme olasılıkları zayıflar.

Sayım aşamasındaki zorluk, özünde saymanın güvenilirliğidir. Kullanılan oylar kamuya açık olsa da seçmenlerden bazılarının bunu denetlemeyeceği düşüncesiyle saymanın kullanılan oyları farklı yayınlaması ve bunun fark edilmemesi olasılığı olabilir. Bu soruna önerilecek en mantıklı çözüm, saymanların sayısının artırılmasıdır. Böylece birbirini karşılıklı denetleyen saymanların varlığıyla sayım güvenilir duruma getirilir.

Bundan başka, saymanlarla konaklar arasındaki ağda anonim iletişim yapılamaması durumunda bireysel olarak kullanılan konakların gönderdikleri oylar ağ ters yönde izlenerek seçmenle eşleştirilebilir. Sayman sayısının birden fazla olması da ters yönde izlemeyi zorlaştıracak yöntemlere yardımcı olacaktır.

Yukarıda söz edilen sorunlarla başa çıkabilmek için, dizgede daha önce sözü edilmeyen iki özelliğin daha eklenmesi önerilir: oy verme işleminin denetlenen merkezî konaklarda gerçekleştirilmesi ve birden fazla bağımsız sayman olması.

Oy verme işlemi denetlenen merkezî konaklarda gerçekleştirildiği durumda oy satılması ve etmenleri bozma olasılıkları azalacaktır. Bunun yanında, her seçmenin

vermiş olduğu oyu denetlemesi dizgenin bir parçasıdır. Bu durumda, seçmenlere kullandıkları oyu ya da oylarıyla eşleşen rastgele sayıyı gösterir bir fiş verilebilir. Fiş vermek de oy satılması konusunda daha önceki sorunla aynı durumu yaratacağından verilen fişlerin de oyu ya da rastgele sayıyı açıkça belirtmeyecek bir yolla hazırlanması gerekecektir[14]. Bu yol, seçmenler kabin içindeyken kullandıkları oyu açıkça gösteren ama kabinden çıkınca bozulan bir fiş üretmektir. Bu durumda, seçmenler oy verme anında kullandıkları oyu denetlediklerinden daha sonra denetlemek üzere şifrelenmiş oyların özünü saklamaları gerekmeyecektir.

Sayımın güvenliğini artırmak için yetkenin anahtarının yanı sıra karşılıklı birbirlerini denetlemeleri için sayılarının birden çok olduğu düşünülen her bir saymanın açık anahtarı ile ardarda şifrelenen oy pusula etmeninde saklanacaktır. Bu karıştırıcı ağ yapısı ilkesine yakın bir yaklaşımdır ve kolaylıkla bir karıştırıcı ağ altyapısına dönüştürülebilir. Böylece, herhangi bir tarafın hile girişimi kolaylıkla ortaya çıkarılabilir. Bunun yanında, karıştırıcı ağ altyapısı seçmenlerin ağ trafiği izlenerek tanınmasını da engelleyecektir.

4.2.3 Var olan dizgelerle karşılaştırma

Yukarıdaki paragraflarda eklenen özellikleriyle birinci öneriyi var olan dizgelerle karşılaştırdığımızda, diğer dizgelerin uygulamada karşılaştığı zorlukların birçoğunun üstesinden gelindiğini görebiliriz.

Öncelikle, önerilen dizgenin en büyük getirisi etmen tabanlı olmasıdır. Etmen tabanlı dizgenin içerdiği sunucuların gerçek zamanda hesaplama yapma gereğinden kurtulması, hesaplamaların sadece seçmenin oy kullandığı konaklarda gerçekleştirilmesi sunucular için tutumlu yatırımların yeterli olacağını gösterir.

Bunun yanında, daha önce gerçekleştirilen oylamaların önemli sorunlarından olan oylama yazılımlarının denetimine ve güncellenmesine ilişkin sorunlar[4] tam anlamıyla ortadan kalkacaktır.

Oylama yapılan konakların yetkisizce ya da hile amaçlı değiştirilmesi tehlikesi etmenler kullanıldığında konağın doğrudan etmene etki edememesi nedeniyle daha az tehlikeli olacaktır.

Var olan karıştırıcı ağ tabanlı dizgelerin eksiği, söylendiği gibi görece yavaş işlemeleriydi. Önerilen dizgede hesaplamalar seçmenin oy verme işlemini

gerçekleştirdiği konakta yapılacağından sunucu hızları görece önemsizleşmektedir. Tek bir seçmen için yapılan hesaplamanın da günümüz bilgisayarları için oldukça sıradan işlemler olduğu düşünüldüğünde dizgenin hızının büyük ölçüde sunucularla konaklar arasındaki bant genişliğiyle ilgili olduğu görülür. Dizgenin sayım aşamasında karıştırıcı ağ altyapısını kullanması ise görece önemsizdir. Daha önce de belirtildiği gibi, sayım çevrimdışı yapılacaktır.

Eş işlem tabanlı dizgelerin eksiği olan önceden belirlenmiş seçenekler dışında oy kullanamama özelliği, körleştirme tabanlı bir yaklaşım seçildiğinden önerilen dizgede var olmayacaktır.

Körleştirme tabanlı yaklaşımın eksiği olan sayman ile konak arasında anonim iletişim gerekliliği ise önerilen dizgede de var olmakla birlikte, merkezî konakta çok sayıda seçmen oy kullanacağı için oylar ile seçmenler arasında birebir eşleme olanağı kalmayacaktır. Yanı sıra, karıştırıcı ağ altyapısına benzer sayman altyapısı kullanılırsa trafiğin izlenmesi tehlikesi ortadan kalkacaktır.

4.3 İkinci Yöntem

Bu yöntem bilinen körleştirme tabanlı yaklaşımı etmenlere uyarlamayı deneyen yaygın çevrimdışı elektronik oylama dizgesiyle gerçekleştirilebilir. Yöntem üç taraf içerir. Taraflardan ikisinin uzantısı olacak etmenler tasarlanmıştır. Bu etmenler üçüncü tarafa ilişkin bilgisayarda çalışarak hesaplamaları yapacak ve oy verme işlemini tamamlayacaklardır.

İlk önerinin aksine, bu yöntem yaygın elektronik oylama dizgesini barındırmak üzere hazırlanmıştır. Ayrıca, bu yöntemde bir seçmen oylama süresi sonuna kadar oyunu değiştirebilecektir. Bu yolla oy satılması tehlikesinin önüne geçilmiştir.

4.3.1 Dizgenin İşleyişi

Dizgenin işleyişindeki değişiklikler kayıt aşamasını yeni bir açık anahtarın daha seçmene teslim edilmesi gereği dışında etkilemeyecektir. Kayıt aşamasının ardından gelen oy verme aşamasında ve sayım aşamasında değişiklikler vardır. Kullanılacak olursa oy değiştirme aşaması oy verme aşaması ile sayım aşamasının arasına eklenecektir.

Bu dizgede önerilen ilk dizgedeki anahtarların yanında oy değiştirme aşamasında kullanılan yetkeye ilişkin bir anahtar çiftine daha gereksinim vardır. Yetkeye ilişkin ilk anahtar çifti oy yaratılmasında kullanılacakken, yetkeye ilişkin diğer anahtar çifti verilen bir oyu değiştirmeye yarayacaktır. Bu anahtar çiftine bölüm boyunca *oy değiştirme anahtar çifti* olarak değinilecektir.

Bu dizgede kullanılacak etmenlerin yapısında da bir değişiklik gerekecektir. Her bir etmen oy verme aşamasında mı, oy değişikliği aşamasında mı olduğunu bilmelidir. Etmenler her iki aşamada farklı davranacaklardır. Bu nedenle etmenlere bunu bildiren bir alan eklenmelidir.

Seçmenlerin kaydının ardından oylama sırasında gerekli olan etmenler çevrimdışı hazırlanırlar. Oy değiştirme işleminin sık yapılmayacağı düşünülerek sadece oy verme durumundaki etmenler önceden hazırlanır. Oy değiştirmekle görevli etmenlerin gerekli olduklarında gerçek zamanda hazırlanacakları varsayılmıştır.

Oy verme aşaması benzer şekilde başlayacaktır. Yetkeye gönderilen iki parçalı bir ileti oy verme işlemini başlatır. Yetkenin gönderdiği defter etmeni seçmenin oy kullandığı konakta çalışarak pusula etmenini alır ve etkinleştirir. Pusula etmeni seçmenin oyunu bir rastgele sayıyla bitiştirerek körleştirir ve defter etmenine gönderir. Defter etmeni körleştirilmiş oyu yetkenin gizli anahtarıyla şifreleyerek pusula etmenine gönderir ve sonlanır. Pusula etmeni ters körleştirme işlemiyle şifrelenmiş oyu elde ettikten sonra bunun özünü alır ve bu özü konakta saklar. Daha sonra oyu saymanın açık anahtarlarıyla şifreler. Bunu saymana ilettikten sonra pusula etmeni sonlanacaktır. Yetkeye gönderilen bir onay iletisiyle oy verme aşaması biter.

Oy değiştirme aşamasının başlangıcı da benzerdir. Seçmen iki parçadan oluşan bir iletiyle oy değiştirme aşamasını başlatır. Seçmen oy değiştirmek için göndereceği iletide yetkenin açık anahtarı yerine oy değiştirme açık anahtarını kullanacaktır. Seçmenin oy değiştirmek istediğini anlayan yetke seçmenin kayıtlı olup olmadığını, daha önceden oy kullanıp kullanmadığını denetleyerek seçmenin durumu uygunsa yeni bir defter etmeni yaratarak gönderecektir. Yaratılan yeni defterin içeriğinde yetkenin gizli anahtarı yerine oy değiştirme gizli anahtarı bulunacaktır. Defter etmeni başarılı bir şekilde seçmenin oy kullanacağı konağa göçtükten sonra pusula etmenini alır ve etkinleştirir. Pusula etmeni oyu rastgele bir sayıyla bitiştirip körleştirdikten sonra defter etmenine gönderir. Daha sonra defter etmeninden gelen iletiyi ters körleştirme işlevinden geçirerek şifrelenmiş oyu elde eder. Daha önce gönderilen oya

ilişkin özü okuyarak şifrelenmiş oya bitiştirir. Bu oyun özünü alıp bir önceki özün yerine koyduktan sonra oyu saymanın açık anahtarıyla şifreler. Bu oyu saymana gönderdikten sonra sonlanır. Seçmen oy değiştirme işlemini bitirdiğine dair bir onay iletisini yetkeye yollayarak işlemi sonlandırır.

Sayım aşamasında sayman ilk olarak kendi açık anahtarıyla kendisine iletilmiş tüm iletilerin şifresini çözer. Elde ettiği yeni verilerin özlerini alarak bir öz listesi oluşturur. Değiştirilmiş olarak işaretlenen oylara bitişik bulunan özlerin yeni oluşturduğu listede olup olmadığını denetler. Eğer bu öz geçerli değilse bitişiğindeki oyu ve o iletiye ilişkin özü; bu öz geçerliyse özün eşlemi olan (mapped) oyu siler. Özleri karşılaştırarak yapılan bu süzme işleminin sonunda saymanın elinde sadece geçerli oylar ve hem kullanılanlar hem de değiştirilenlerinki dahil olmak üzere tüm geçerli oyların özleri kalır. Sayman geçerli olarak kullanılmış ya da değiştirilmiş oyları gösteren bir öz listesini yayınlar.

Oy verme aşamasının içerdiği adımlar aşağıda özetlenmiştir. Her bir adımın güvenliği ile ilgili irdeleme ayrıt 4.3.2.1'de verilmiştir. Oy verme aşamasını gösteren UML **Şekil 4.10**'de verilmiştir.

i. Seçmen oy verme işlemini başlatmak üzere yetkeye *"$Şifreleme_{YetkeAçıkAnahtar}(KimlikNo)||Şifreleme_{SeçmenGizliAnahtar}(KimlikNo)$"* iletisini gönderir.

ii. Yetke iletinin ilk parçasını okuduktan sonra seçmene ilişkin açık anahtarla ikinci parçayı açmayı dener. Eğer iletinin iki parçası birbirine denkse kayıtlı seçmenler arasında seçmeni arar. Seçmen kayıtlı değilse işlem iptal edilecektir. Seçmen oy kullanan seçmenler arasında aranır. Henüz oy kullanmadığı belirlenirse oy kullanma işlemi uygun şekilde başlatılır. *"$Şifreleme_{SeçmenAçıkAnahtar}(OturumAnahtarı)||Şifreleme_{OturumAnahtarı}(Defter)$"* iletisi seçmene gönderilir. Seçmen oy kullanmışsa işlem sonlandırılır.

iii. Seçmen gelen iletinin şifresini uygun biçimde çözerek defter etmenini çalıştırır. Defter etmeni saymandan pusula etmenini ister. Pusula etmenini saymanca imzalanmış olarak alan defter etmeni pusula etmenini etkinleştirir.

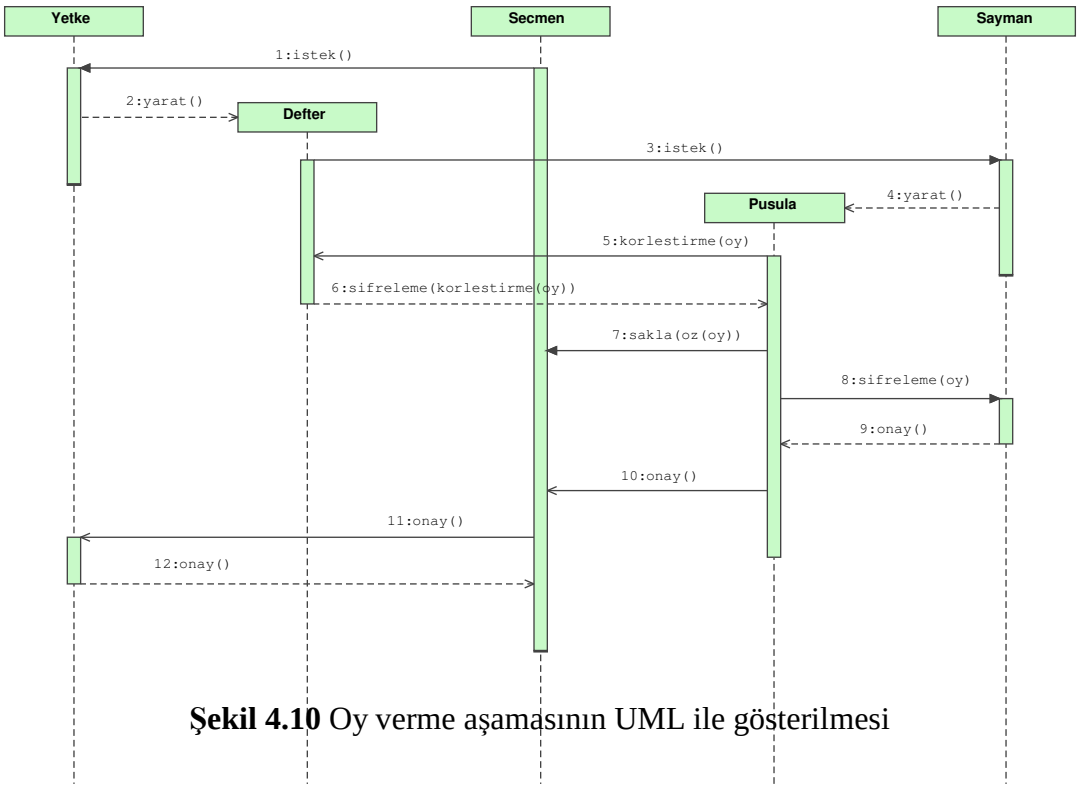
iv. Pusula etmeni seçmenin kendisine ilettiği oyu bir rastgele sayıyla birleştirdikten sonra körleştirir. *"$Körleştirme_{KörleştirmeÇarpanı}(Oy||RastgeleSayı)$"* iletisini defter etmenine gönderir.

v. Defter körleştirilmiş oyu yetkenin gizli anahtarıyla şifreler. *"$Şifreleme_{YetkeGizliAnahtar}(Körleştirme_{KörleştirmeÇarpanı}(Oy||RastgeleSayı))$"* iletisini pusulaya gönderdikten sonra sonlanır.

vi. Pusula iletiyi ters körleştirme işlevinden geçirerek *"$Şifreleme_{YetkeGizliAnahtar}(Oy||RastgeleSayı)$"* sayısını elde eder. Pusula bu sayının özünü alarak saklar. Pusula bu sayıyı saymanın açık anahtarıyla şifreler. *"$Şifreleme_{SaymanAçıkAnahtar}(Şifreleme_{YetkeGizliAnahtar}(Oy||RastgeleSayı))$"* iletisini saymana gönderip kendini sonlandırır.

vii. Seçmen iki parçadan oluşan bir onay iletisi oluşturur. Oluşturduğu *"$Şifreleme_{YetkeAçıkAnahtar}(KimlikNo)||Şifreleme_{SeçmenGizliAnahtar}(Onay)$"* iletisini yetkeye gönderir.

viii. Yetke uygun şekilde şifresini çözdüğü iletinin anlamlı olması durumunda seçmeni oy kullanmış olarak imler.



Şekil 4.10 Oy verme aşamasının UML ile gösterilmesi

Oy değiştirme aşamasının içerdiği adımlar aşağıda özetlenmiştir. Her bir adımın güvenliği ile ilgili irdeleme ayrıt 4.3.2.2'de verilmiştir. Oy değiştirme aşamasını gösteren UML **Şekil 4.11**'de verilmiştir.

i. Seçmen oy verme işlemini başlatmak üzere yetkeye *"Şifreleme$_{OyDeğiştirmeAçıkAnahtar}$(KimlikNo)||Şifreleme$_{SeçmenGizliAnahtar}$(KimlikNo||R)"* iletisini gönderir. KimlikNo verisi şifrelenirken sonuna anlamsız rastgele veriler eklenir.

ii. Yetke iletinin ilk parçasını okuduktan sonra seçmene ilişkin açık anahtarla ikinci parçayı açmayı dener. Eğer iletinin iki parçası birbirine denkse kayıtlı seçmenler arasında seçmeni arar. Seçmen kayıtlı değilse işlem iptal edilecektir. Seçmen oy kullanan seçmenler arasında aranır. Henüz oy kullanmadığı belirlenirse işlem sonlandırılır. Eğer seçmen oy kullanmış ise oy değiştirme işlemi uygun şekilde başlatılır ve *"Şifreleme$_{SeçmenAçıkAnahtar}$(OturumAnahtarı)||Şifreleme$_{OturumAnahtarı}$(Defter)"* iletisi seçmene gönderilir.

iii. Seçmen gelen iletinin şifresini uygun biçimde çözerek defter etmenini çalıştırır. Defter etmeni saymandan pusula etmenini ister. Pusula etmenini saymanca imzalanmış olarak alan defter etmeni pusula etmenini etkinleştirir.

iv. Pusula etmeni seçmenin kendisine ilettiği oyu bir rastgele sayıyla birleştirdikten sonra körleştirir. *"Körleştirme$_{KörleştirmeÇarpanı}$(Oy||RastgeleSayı)"* iletisini defter etmenine gönderir.

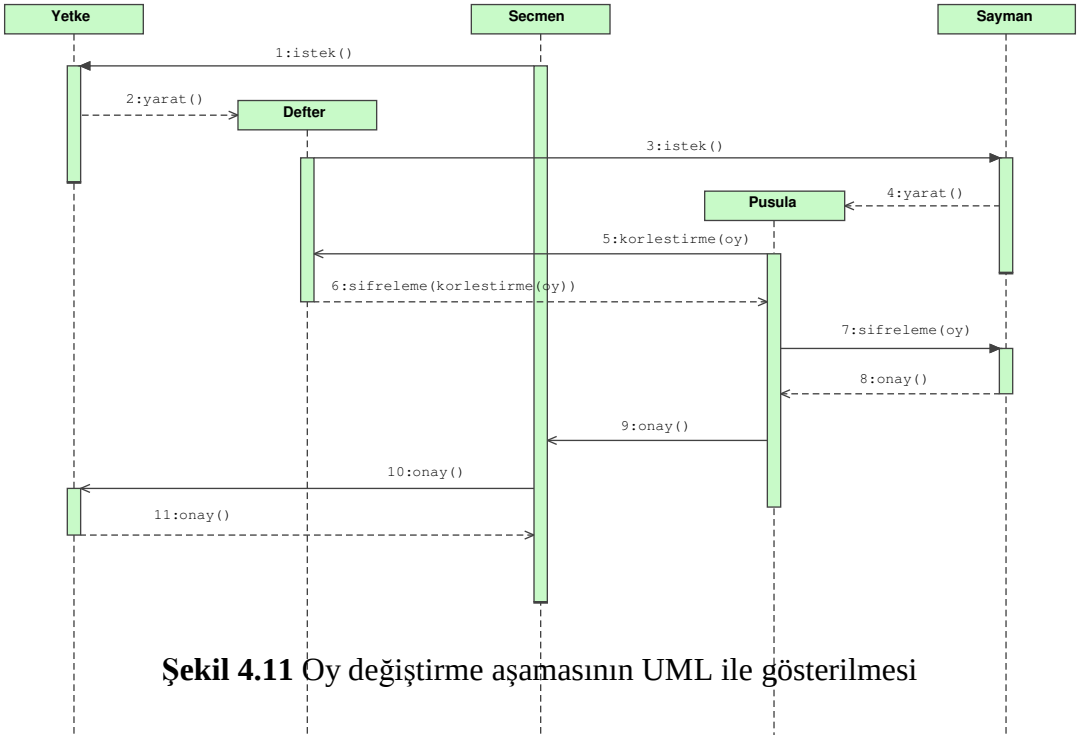
v. Defter körleştirilmiş oyu oy değiştirme gizli anahtarıyla şifreler. *"Şifreleme$_{OyDeğiştirmeGizliAnahtar}$(Körleştirme$_{KörleştirmeÇarpanı}$(Oy||RastgeleSayı))"* iletisini pusulaya gönderdikten sonra sonlanır.

vi. Pusula iletiyi ters körleştirme işlevinden geçirerek *"Şifreleme$_{OyDeğiştirmeGizliAnahtar}$(Oy||RastgeleSayı)"* sayısını elde eder. Pusula daha önceki oya ilişkin özü alarak bu sayıya bitiştirir. Yeni oluşan metnin özünü alarak saklar. Metni saymanın açık anahtarıyla şifreler. *"Şifreleme$_{SaymanAçıkAnahtar}$(Şifreleme$_{OyDeğiştirmeGizliAnahtar}$(Oy||RastgeleSayı)||Öz)"* iletisini saymana gönderip kendini sonlandırır.

vii. Seçmen iki parçadan oluşan bir onay iletisi oluşturur. Oluşturduğu *"Şifreleme$_{OyDeğiştirmeAçıkAnahtar}$(KimlikNo)||Şifreleme$_{SeçmenGizliAnahtar}$(Onay||R)"*

iletisini yetkeye gönderir. Onay verisine şifrelenmeden önce rastgele sayılar bitiştirilmiştir.

viii. Yetke uygun şekilde şifresini çözdüğü iletinin anlamlı olması durumunda seçmeni oy değiştirmiş olarak imler.



Şekil 4.11 Oy değiştirme aşamasının UML ile gösterilmesi

Sayım aşamasının içerdiği adımlar aşağıda özetlenmiştir. Her bir adımın güvenliği ile ilgili irdeleme ayrıt 4.3.2.3'te verilmiştir.

i. Sayman elindeki her bir iletinin şifresini gizli anahtarıyla çözerek yetkenin imzalamış olduğunu varsaydığı *aday oy*ları elde eder.

ii. Sayman *aday oy*ların özlerini alarak yeni bir küme oluşturur. Yeni oluşan *öz*ler kümesi *aday oy*lar kümesiyle birebir eşlenebilir olacaktır.

iii. *Aday oy*lar arasından değiştirilmiş oy olarak işaretli olanlar *aday oy*lar kümesi içinde *değiştirilmiş aday oy*lar altkümesini oluşturur.

iv. *Değiştirilmiş aday oy*ların bitişiğindeki özler, *öz*ler kümesi içinde aranır.

   a. Bulunmaları durumunda özün eşlemi olan oylar geçersiz olarak işaretlenerek *aday oy*lar kümesinden çıkarılırlar.

b. Bulunmamaları durumunda bitişiğindeki *değiştirilmiş aday oy*, *aday oy*lar kümesinden çıkarılır ve bu *aday oy*un eşlemi olan öz, *öz*ler kümesinden çıkarılır.

v. Böylece oylama boyunca kullanılmış geçerli oyların *öz*leri ve değiştirilen oyların dışında kalan geçerli oyları içeren *aday oy*lar kalacaktır.

vi. *Aday oy*lar kümesinin her elemanının şifresi yetkenin açık anahtarıyla çözülerek incelenir. Elde edilen metin anlamlı değilse oy, *aday oy*lar kümesinden ve oyun eşlemi olan öz, *öz*ler kümesinden çıkarılır.

vii. Elde edilen açık metinlerin içeriğine bakılarak oylar sayılır. Özleri içeren küme yayınlanır.

4.3.2 Güvenlikle ilgili irdelemeler

Dizgenin güvenliği irdelenirken sırasıyla oy verme aşamasının güvenliği, oy değiştirme aşamasının güvenliği ve sayım aşamasının güvenliği adım adım incelenecektir. Daha sonra dizgenin güvenliği bir bütün olarak ele alınacaktır.

4.3.2.1 Oy verme aşamasının güvenliği

i. Gönderilen ileti hizmet engelleme saldırılarından yetkenin korunması amacıyla iki parçalıdır. İletinin ikinci parçası seçmen dışında biri tarafından oluşturulamayacağı için yetkenin yanıtladığı tüm iletiler anlamlı olacaktır. İletinin kötü emelli biri tarafından saklanıp yetkeye tekrar gönderilmesi yoluyla yetkenin hizmet vermesini engellemek olanaklı olabilir. Bu nedenle yetke iletiler anlamlı da olsa seçmenlerin başvurularını süzerek sadece gerekli olduğunda yanıtlamalıdır.

ii. Birinci adımda belirtilenlere ek olarak, bu adımda seçmene iletilen etmen bir oturum anahtarıyla, oturum anahtarı da seçmenin açık anahtarıyla şifrelenmiştir. O hâlde, yetkenin gönderdiği etmeni görebilecek tek kişi seçmendir. Defter etmeninin iletimi sırasında ortaya çıkacak hatalı ikililer dolayısıyla seçmenin etmeni tekrar istemesi söz konusu olabilir. Seçmene ilişkin etmen daha önce gönderilmişse, bir kere daha gönderilmesi engellenecektir. Bu durumda, etmenin düzgün taşındığından emin olunması için seçmenden yüklediği etmenin sağlamasını yetkeye göndermesi istenebilir. Seçmenin oy kullanması ile oy değiştirmesi birbirinden ayrılacağından, oy kullanma aşamasının sadece bir kere

gerçekleşeceğinden emin olunmalıdır. Bu durumda, daha önce oy kullandığı görülen bir seçmen bu aşamayı geçemeyecektir.

iii. Pusula etmeninin imzalanmış olması iletişime etki etme olasılığı olan birinin doğru çalışmayan ya da hileli bir pusula etmenini seçmene göndermesini engellemektedir.

iv. Körleştirilmiş oyu körleştirme çarpanını bilmeden görmek olanaklı değildir.

v. Körleştirilmiş oyun yetkenin gizli anahtarıyla şifrelenmesi, körleştirilmiş oyun yetke tarafından imzalanması olarak düşünülebilir. Yetkenin gizli anahtarı etmen içinde taşınsa da kötü emelli birinin buna ulaşmasını engelleyecek yollar önerilebilir. Bu sorunun çözümünde en güvenilen yöntem daha sonra açıklanacak olan kod karmaşası (code mess-up) yöntemidir.

vi. Körleştirildikten sonra imzalanan oy ters körleştirme işlevinden geçirilidiğinde elde edilen imzalanmış oydur. Körleştirme uygulanan işlemleri etkilememiş, sadece oyun okunmasını engellemiştir. İmzalanmış oyun saymanın açık anahtarıyla şifrelenmesi sayman dışında birinin oyu okumasını engeller. İmzalanmış oyun özünün saklanması hem oyun daha sonra değiştirilmesini, hem de seçmen tarafından sayım sonrasında doğruluğunun denetlenebilmesini sağlar.

vii. Hizmet engelleme saldırılarının engellenmesi için birinci adımdakine benzer bir yolla ileti oluşturulmuştur.

viii. Bu adımda güvenlikle ilgili bir açıklama gerekmemektedir.

4.3.2.2 Oy değiştirme aşamasının güvenliği

i. Gönderilen ileti hizmet engelleme saldırılarından yetkenin korunması amacıyla iki parçalıdır. İletinin ikinci parçası seçmen dışında biri tarafından oluşturulamayacağı için yetkenin yanıtladığı tüm iletiler anlamlı olacaktır. İletinin kötü emelli biri tarafından saklanıp yetkeye tekrar gönderilmesi yoluyla yetkenin hizmet vermesini engellemek olanaklı olabilir. Bu sorundan kurtulmak için seçmenin kimlik numarasının sonuna rastgele ikililer eklenerek şifrelenir. Herhangi iki ileti birbirine eş olamayacağından yetke hizmet engelleme saldırılarından korunmuş olur.

ii. Birinci adımda belirtilenlere ek olarak, bu adımda seçmene iletilen etmen bir oturum anahtarıyla, oturum anahtarı da seçmenin açık anahtarıyla şifrelenmiştir.

O hâlde, yetkenin gönderdiği etmeni görebilecek tek kişi seçmendir. Defter etmeninin iletimi sırasında ortaya çıkacak hatalı ikililer dolayısıyla seçmenin etmeni tekrar istemesi söz konusu olabilir. Seçmene ilişkin etmen daha önce gönderilmişse, bir kere daha gönderilmesi engellenecektir. Bu durumda, etmenin düzgün taşındığından emin olunması için seçmenden yüklediği etmenin sağlamasını yetkeye göndermesi istenebilir. Seçmen oy değiştirme işlemini istediği sayıda tekrarlayabileceğinden, daha önce oy değiştirmiş bir seçmen de olsa, defter etmeni gönderilecektir. Ancak, oy kullanmamış bir seçmenin etmeni edinmesi yetke tarafından engellenmelidir.

iii. Pusula etmeninin imzalanmış olması iletişime etki etme olasılığı olan birinin doğru çalışmayan ya da hileli bir pusula etmenini seçmene göndermesini engellemektedir.

iv. Körleştirilmiş oyu körleştirme çarpanını bilmeden görmek olanaklı değildir.

v. Körleştirilmiş oyun yetkenin gizli anahtarıyla şifrelenmesi, körleştirilmiş oyun yetke tarafından imzalanması olarak düşünülebilir. Yetkenin gizli anahtarı etmen içinde taşınsa da kötü emelli birinin buna ulaşmasını engelleyecek yollar önerilebilir. Bu sorunun çözümünde en güvenilen yöntem daha sonra açıklanacak olan kod karmaşası yöntemidir.

vi. Körleştirildikten sonra imzalanan oy ters körleştirme işlevinden geçirilidiğinde elde edilen imzalanmış oydur. Körleştirme uygulanan işlemleri etkilememiş, sadece oyun okunmasını engellemiştir. İmzalanmış oyun saymanın açık anahtarıyla şifrelenmesi sayman dışında birinin oyu okumasını engeller. İmzalanmış oyun özünün saklanması hem oyun daha sonra değiştirilmesini, hem de seçmen tarafından sayım sonrasında doğruluğunun denetlenebilmesini sağlar. Bir önceki oya ilişkin özün saymana gönderilmesiyle sayman geçersizleştireceği oyu belirleyebilecektir.

vii. Hizmet engelleme saldırılarının engellenmesi için birinci adımdakine benzer bir yolla ileti oluşturulmuştur.

viii. Bu adımda güvenlikle ilgili bir açıklama gerekmemektedir.

4.3.2.3 Sayım aşamasının güvenliği

i. Saymanın bu aşamada şifresini çözemediği iletiler geçersiz sayılacaktır.

ii. Dizgede kullanılan öz alma işlevinin oylar arasında çakışma yaratmayacağı varsayılmıştır.

iii. Bu adımda güvenlikle ilgili bir açıklama gerekmemektedir.

iv. Bu adımda güvenlikle ilgili bir açıklama gerekmemektedir.

v. Bu işlemin ardından oylama boyunca kullanılmış geçerli aday oyların özleri ve değişikliklerden sonra geriye kalan geçerli oyları içeren aday oylar kalacaktır.

vi. Yetke tarafından imzalanmamış herhangi bir oyun sayılması engellenmiştir.

vii. Özleri içeren kümenin yayınlanmasıyla her bir seçmen kullandığı oyun sayım sırasında işlendiğinden emin olacaktır.

4.3.2.4 Dizgenin güvenliği

Bu dizgenin bireyselliği daha önce değinildiği gibi, ancak kayıt aşamasından sonra incelenebilir. Bireyselliğin sağlanmasındaki bir başka sorun olarak seçmenin kendine ilişkin anahtarı kaybetmesi ya da bir başkasına vermesiyle ortaya çıkabilir. Ne yazık ki, seçmenin bireysel olarak anahtarını saklama yükümlülüğünde olduğunu düşünmek dışında bir çözüm biyolojik temellere dayanan asıllama yöntemlerine başvurulmadıkça görünmemektedir. Dizgenin bireyselliğini sağlayan temel, sadece seçmende var olan gizli anahtarla açılabilecek bir yolla defter etmeninin seçmene gönderilmesiyle sağlanır. Böylece asıllanmamış birinin defter etmenini çalıştırması olanaksızlaştırılır.

Dizgenin tekilliği, yani kaydolmuş her bir seçmenin sadece tek bir kere oy kullanması, sayman tarafından geliştirilen yaklaşımlarla çözülecektir. Sayman sadece uygun biçimde oluşturulmuş ya da seçmenlerce uygun biçimde değiştirilmiş oyları kabul edecektir.

Dizgenin kesinliğini sağlayan temel oyların ancak ve ancak doğru biçimde oluşturulduklarında anlamlı olarak sayılabilmeleridir. Gerçekten var olmayan bir rastgele oy oluşturulması denenirse, sayım aşamasında dizge için anlamsız bir veri olacağı için bu oy önemsenmeyecektir. Gerçekte, böyle bir rastgele oyun oluşturulması da olanaklı değildir, çünkü oylarla birebir eşleştirilmiş özler sayım sırasında incelenmektedir. Oluşturulan bir oyun saklanmasının ardından üzerinde yapılacak yöntemli bir değişiklikle başka bir oya dönüştürülmesi olanağı şifrebilimsel ilkeler sayesinde yoktur.

Dizgenin bütünlüğü iki ayrı yolla sağlanabilir. Birincisi, bir oyun sezilmeden silinmesini engeller. Yetke tarafından onaylanmış oyların sayısı ile sayman tarafından açıklanan oyların sayısı birbirini tutmalıdır. İkincisi, bir oyun hem silinmesini, hem de değiştirilmesini engeller. Değinildiği gibi, seçmenler kullandıkları oyları saymana göndermeden önce özlerini almışlardır. Seçmenler bu özü saymanın yayınladığı özler listesiyle karşılaştırarak oyunun doğru biçimde sayıldığını görebilir.

Dizgenin sayımı açık ve ancak saymanların dürüst birlikteliğiyle yapılacağından her aşamasında denetlenebilirliği sağlanmıştır.

Dizge etmen tabanlı olduğundan bağlantı sorunlarından en az etkilenecek yapıdadır. Etmenlerin düzgün taşınmaması olasılığı da etmenlerin taşınmalarının ardından bütünlük denetiminden geçmeleriyle önlenmiştir.

Seçmenlerin kullandıkları oyların açığa çıkmaması, yani gizlilik, her seçmen tarafından yaratılan ve körleştirme için de kullanılan rastgele sayıya bağlıdır. Her bir seçmen kendine ilişkin oyu kendi yarattığı bir rastgele sayıyla tanıyabilir. Bu sayı sadece oy verme işlemi sırasında kullanıldığından ve bu işlem sırasında rastgele sayının yetkeye taşınması olasılığı olmadığından dizgenin gizliliği sağladığı görülür. Bu rastgele sayı bir kurala bağlı olarak oluşturulmadığından herhangi birinin rastgele sayıya bakarak seçmenin kimliğini öğrenmesi düşünülemez.

Yukarıdaki paragraflarda bir elektronik oylama dizgesinin sağlaması gereken koşulları sağlasa da dizgenin uygulanması sırasında karşılaşılabilecek olası sorunlardan söz edilebilir. Bu sorunlar da ilerleyen paragraflarda ayrıntılarıyla tartışılmıştır.

Dizgenin uygulanmasında karşı karşıya kalınacak sorunların ilki, daha önce de söz edildiği gibi kayıt aşamasında ve oy verme işlemi sırasında biyolojik temelli asıllamanın getirdiği zorluktur. Biyolojik temelli asıllama kullanılmadıkça kayıt aşamasında geçerli seçmenlerin kaydedildiğinden emin olmak güçtür. Oy verme işlemi sırasında da kayıt aşamasındakine benzer şekilde seçmenlerin biyolojik temelli asıllama yöntemleri uygulanmadıkça asıllanmalarında zorluklar çıkmaktadır.

Seçmenlerin sahip oldukları konaklarda ya da bir konağa sahip olmamaları durumunda merkezî konaklarda oy kullandığı düşünülebilir. Merkezî ve görevlilerce denetlenen konaklarda oy kullanılması sırasında asıllamanın güvenliği bir nebze

artmış olacaktır. Oysa, seçmenlerin kendilerine ilişkin konaklarda oy kullandığı düşünüldüğünde asıllamayı tam anlamıyla denetlemek olanaklı değildir. Buna rağmen, dizgenin yaygın çalışması sırasında kullanabileceği yöntemler vardır. Defter etmeni asıllamayı sağlamak üzere, yetke tarafından bilinen ve ancak bireysel olarak yanıtlanabileceği düşünülen bir dizi sorunun yanıtının özünü içerecek şekilde tasarlanabilir. Sözü edilen sorular seçmenin annesinin kızlık soyadı, amcasının kızının adı ya da nüfusa kayıtlı olduğu mahalle gibi kişiselleştirilmiş sorular olmalıdır. Bunun yanında seçmen şifreleri ya da akıllı kartların kullanımı da çözüme yardımcı olacaktır.

Oy verme aşamasında da iki sorunla karşılaşılır. Birincisi oy satılması tehlikesidir. Neyse ki, dizgeye dahil olan her seçmenin verdiği oyu değiştirme hakkı saklıdır. Bu durumda bir seçmeni oy verme aşamasında izleyen kötü niyetli birinin oy satın alması zordur çünkü izleyen kişinin seçmenin yanından ayrılmasının ardından seçmen oyunu değiştirip gerçekte istediği partiye oy verebilir.

Oy verme aşamasında karşılaşılan ikinci tehlike yine seçmenlerin bağımsız konaklarda oy kullanması durumunda karşılaşılacak olan zorluklardan biridir. Etmen tabanlı yöntemin önerilmesi, temelde, etmenlerin güvenli bir şekilde devinebilecekleri altyapıya sahip bir ortamı gerektirecektir. Bu ortamı sağladığını iddia eden altyapı seçenekleri varsa da denetlemeye kapalı bir konağın güvenliğinden haklı olarak şüphe edilebilir. Etmenlerin güvenliğiyle ilgili en ciddi tehlike, yetkeye ilişkin gizli anahtarı beraberinde taşıyan defter etmeninden bu anahtarın alınmasıdır. Bu anahtarın ele geçmesi ile sahte oylar yaratılabilir. Her ne kadar sahte oy eklendiği dizge tarafından fark edilse de, hangi oyların eklendiğini fark etmek olanaklı olmayacaktır. Bir yaygın elektronik oylama dizgesinde bunu çözecek iki yaklaşımdan söz edilebilir.

Birincisi, etmen altyapılarının etmenler tarafından etkinleşmelerinden hemen önce denetlenmesidir. Önerilen dizgedeki kayıt aşamasının varlığı bunu görece kolay kılmaktadır. Bir rastgele sayı dışında birbirinin aynısı olan etmen altyapıları hazırlandıktan sonra bu etmenler kayıt sırasında seçmenlerle birebir eşleştirilebilir. Defter etmeni etkinleşmesinden hemen önce göçtüğü etmen altyapısının özünü alarak kendi kayıtlarındakiyle örtüşüp örtüşmediğini denetleyebilir.

İkinci yöntem Hohl tarafından önerilen kod karmaşası yöntemidir. [29] Bu yöntemde etmenin kodu bir yazılım yardımıyla salık verilen tasarım kalıplarınca belirlenen

kuralların tam aksine okunamayacak derecede karıştırılır; işlevler çok küçük parçalara ayrılır ya da tamamen ortadan kaldırılır, kullanılan verilerin yanına pek çok anlamsız veri eklenir, veriler değişik boyutlu ve değişik türde diziler ya da veri yapıları içine gömülür, anlamsız işler yapan işlevler eklenir. Böylece gerçekte aynı işi yapan ama hem kaynağı hem de derlenmiş şekli okunamayacak derecede karmaşıklaştırılmış yazılım parçaları üretilebilir. Yöntemin ilkesi, belirli bir süre içinde okunamayacak kadar karmaşıklaştırılmış kodlar oluşturmaktır. Yöntemin kötü yanı bellek ve işlem iyileştirmelerinin uygulanamaması nedeniyle yavaş çalışan kodlara neden olmasıdır. Dizgemizdeki etmenler seçmenlerin konaklarında ve olasılıkla yeterince kaynağa sahip olarak çalışacaklardır. Bu durumda kaynakların kötü kullanımı önemli bir götürü değildir. Bunun yanında, bir oylamanın süresi en fazla bir kaç saat olacağından bu yöntemle üretilen etmenlerin dizgemizde oylaa süresince bozulmadan kullanılabileceği düşünülmüştür.

Ayrıca, bu iki yöntemin bir arada kullanılması, hatta bilinen diğer yöntemlerle[30] birleştirilerek güçlendirilmesi olanaklıdır.

Sayım aşamasındaki zorluk, özünde saymanın güvenilirliğidir. Kullanılan oylar kamuya açık olsa da seçmenlerden bazılarının bunu denetlemeyeceği düşüncesiyle saymanın kullanılan oyları farklı yayınlaması ve bunun fark edilmemesi olasılığı düşünülebilir. Bu soruna önerilecek en mantıklı çözüm, saymanların sayısının artırılmasıdır. Böylece birbirini karşılıklı denetleyen saymanların varlığıyla sayım güvenilir duruma getirilir.

Bundan başka, saymanlarla konaklar arasındaki ağda anonim iletişim yapılamaması durumunda bireysel olarak kullanılan konakların gönderdikleri oylar ağ ters yönde izlenerek seçmenle eşleştirilebilir. Sayman sayısının birden fazla olması trafiği izlemeyi engelleyecektir.

Her bir oyun bir sayman yerine her bir saymanın anahtarı ile rastgele sırada şifrelendiği düşünülebilir. Oyların kötü niyetli bir sayman tarafından içeriğine bakılmaksızın silinmesini engellemek üzere her seçmen belirlenen sayıda saymandan ya da daha fazlasından oyunun ulaştığına dair onay alır. Saymanlar ellerinde bulunan şifrelenmiş oyların içinde kendi anahtarlarıyla açabilecekleri oyları açarlar ve diğer oyları açabilecek saymanlara iletirler. Bu işlem sayman sayısı kere tekrarlandıktan sonra her bir saymanda gönderilen tüm oylar şifreleri çözülmüş olarak bulunacaktır. Böylece her bir sayman diğerlerinden bağımsız olarak sayım yapıp sonuçları

açıklayabilir. Kötü niyetli bir saymanın trafiği izleyerek şifrelenmiş bir oyla bir seçmeni ilişkilendirmekte başarılı olması durumunda dahi bütün diğer saymanlarla ortaklık yapmadığı sürece hangi oyun hangi seçmene ilişkin olduğunu bulması olanaklı olmayacaktır. Bu yapı bir çok özelliğiyle karıştırıcı ağ yapısını andırmaktadır.

Dizgenin hizmet engelleme ve tekrar saldırılarına karşı güvenilirliğini sağlamak amacıyla tekrar gönderilmesi ve sunuculardan yanıt alınması olanaklı görünen iletiler, örneğin oy değiştirme aşamasını başlatan iletiler, şifrelenmeden önce verinin arkasına anlamsız ikililer eklenerek oluşturulmuştur. Bu yolla hizmet engelleme amaçlı tekrar saldırılarının önüne geçilebilir.

Tüm bunların dışındaki bir saldırı, bir önceki oylamada ağ trafiğinde kaydedilmiş verilerin kötü niyetli kişilerce saymanlara ya da yetkeye tekrar gönderilmesi biçimindeki bir tekrar saldırısı olabilir. Bu saldırı bir önceki oylamanın sonuçlarından hoşnut olan bir topluluk tarafından denenebilir. Her oylama için yetke ve saymanlar tarafından yeni anahtarlar yaratılması sorunu çözecek yaklaşımlardan biriyken, dizge içinde oluşturulan iletilere zaman damgası eklenmesi günlük tutmada da yararlı olabilecek bir başka çözümdür. Bu iki çözümün bir arada kullanılması da olanaklıdır.

4.3.3 Var olan Dizgelerle Karşılaştırma

İkinci önerimizi var olan dizgelerle ve ilk önerimizde sunduğumuz dizgeyle karşılaştırdığımızda sorunların birçoğunun aşılmış olduğu görülür.

Önerilen bu dizgenin de ilk önerimizdeki gibi etmen tabanlı olması ve çevrimdışı hesaplamalarla işleyebilmesi en önemli getirileridir. Etmen tabanlı dizgenin içerdiği sunucuların gerçek zamanda hesaplama yapma gereğinden kurtulması, hesaplamaların sadece seçmenin oy kullandığı konaklarda gerçekleştirilmesi sunucular için tutumlu yatırımların yeterli olacağını gösterir. Etmenlerin ortamdan ortama taşınmasındaki kolaylıklar, özellikle bir yaygın elektronik oylama dizgesinde, geniş çapta kullanılabilirliği gösterir.

Bunun yanında, daha önce gerçekleştirilen oylamaların önemli sorunlarından olan oylama yazılımlarının denetimine ve güncellenmesine ilişkin sorunlar[4] tam anlamıyla ortadan kalkacaktır.

Oylama yapılan konakların yetkisizce ya da hile amaçlı saldırılarına karşı, özellikle belirlenen güvenlik önlemleriyle donatıldıktan sonra, kullanılan etmenler seçmenin ya da konağın doğrudan etkisinden uzak çalışacak ve seçmenlerin davranışlarını sınırlanan kalıplar içinde tutabilecektir.

Karıştırıcı ağ tabanlı dizgeleri andırır bir yöntemle sayım yapılıyor olsa da, önerilen dizge çevrimdışı çalışacağından karıştırıcı ağların kötü tarafı olan yavaşlık dizgeyi görece daha az etkileyecektir.

Eş işlem tabanlı dizgelerin eksiği olan önceden belirlenmiş seçenekler dışında oy kullanamama özelliği, körleştirme tabanlı bir yaklaşım seçildiğinden önerilen dizgede var olmayacaktır.

Körleştirme tabanlı yaklaşımın eksiği olan sayman ile konak arasında anonim iletişim gereği ise önerilen dizgede sadece saymanın tek bir konakta olması durumunda fark edilecektir. Dizge yapısı gereği çok sayıda bağımsız saymana izin vermektedir. Saymanlardan birinin güvenilir olması, ağ trafiğinin izlenmesi yoluyla oylarla seçmenleri eşleştirmeyi olanaksız kılar.

Önerilen dizgede sunucu olarak değerlendirilebilecek olan yetke ve sayman tarafları hesap yapmaktan daha çok dosya sunucusu gibi çalışacaklardır. Bu durumda, veri tabanında gerçekleşen sorgu süreleri de önemsenmezse, sunucuların verimliliği sunucuların hızından çok sunucular ile seçmenler arasındaki bant genişliği ile belirlenecektir. Daha sonraki bölümde görüleceği gibi, gerçeklenmiş etmenlerin boyu dar bant genişliği olan bir ağda dahi birkaç saniye içinde göçmelerini sağlayacak kadar küçüktür.

5 BENZETİM

Önerilen dizgelerin gerçeklenebilirliğini göstermek amacıyla yerel ağ üzerinde çalışacak bir benzetim hazırlanmıştır. Birinci yöntemin ikinci yöntem tarafından kapsandığı düşünülerek sadece ikinci yöntemin benzetimi anlatılacaktır. Benzetim yetke, sayman ve seçmen olmak üzere üç taraf içermektedir. Sayman ve yetke tarafı benzetimin basitleştirilmesi adına sadece birer konak içerecek şekilde oluşturulmuştur. Seçmen tarafı konak sayısı değişebilir. Önerilen dizgeden farklı olarak, saymana ulaşan her oyun ardından sayım yapılmakta ve konağın ekranında sonuç gösterilmektedir.

Benzetim oluşturulurken olabildiğince basit bir etmen altyapısı oluşturulmuş ve bu yapının bazı yerleri benzetime bir katkısı olmayacağı düşünülerek eksik bırakılmıştır. Benzetimin önerilen dizgeden eksik olan yanları şöyle sıralanabilir; kod karmaşası yöntemi kullanılmamıştır, hizmet engelleme saldırılarına karşı güvenlik önlemleri yoktur ve etmen altyapısı etmenler tarafından tanınmamaktadır. Bundan başka, diğer etmen altyapılarında var olmasına alışılmış etmen erişim hakları da tanımlanmamıştır.

Önerilen dizge Java programlama dili kullanılarak kolaylıkla gerçeklenmiştir. Benzetimde bakışımsız şifreyazım için RSA algoritması, bakışımlı şifreyazım için TripleDES algoritması, öz alma için SHA1 algoritması ve rastgele sayılar için Java dilinin sağladığı "SecureRandom" sınıfı kullanılmıştır. Gerçeklenen dizgedeki şifrebilimsel algoritmaların, öz alma işlevlerinin ve rastgele sayı üreteçlerinin ideal olduğu varsayılmıştır.

Benzetimde kullanılan RSA algoritmasıyla birlikte kullanılabilecek, anlatılan özelliklere sahip uygun bir körleştirme algoritmasına da gerek duyulur. Kullanılan algoritma şu şekilde çalışmaktadır: Pusula etmeni rastgele bir körleştirme çarpanı, '*k*' oluşturur. '$x=((o||r)k^e)_n$' sayısı yetkenin açık anahtarı '*(n,e)*' kullanılarak oluşturulmuştur. '*o*' sayısı seçmenin kullandığı oyu, '*r*' sayısı rastgele bir sayıyı belirtir. '*x*' defter etmenine gönderilir. Defter etmeni yetkenin gizli anahtarı olan '*(n,d)*'yi kullanarak '$y=(x^d)_n=((o||r)^d k)_n$' sayısını hesaplayıp pusula etmenine

gönderir. Pusula etmeni '$(y/k)_n=((o||r)^d)_n$' hesabını yaparak imzalanmış oyu elde eder.

Benzetimde yetke tarafında defter etmeninin dışında, her bağlantıyı eşzamanlı bir işle ilişkilendiren sınıflar yaratan bir sunucu sınıfı vardır. Bunun dışında, anahtar yaratmaya yarayan sınıflar ve seçmenlere özel defter etmenlerini oluşturmaya yarayan sınıflar vardır. Bu sınıfların işlevlerinin çalışma zamanını ölçen ve sunucu kayıtlarını tutan iki sınıf bunlara eşlik eder.

Sayman tarafında pusula etmeni, bundan başka pusula etmenini oluşturmaya yarayan bir sınıf, anahtar yaratmaya yarayan bir sınıf, sunucu ve her bir bağlantının eşlendiği alt sunucu sınıfları, sayılan oyları gerçek zamanda gösteren bir arayüz ve yetke tarafında da olduğu gibi kayıt tutan ve zaman ölçen sınıflar bulunur.

Seçmen tarafı diğerlerine kıyasla daha sade görünür. Gerçekte de olması gereken bundan farklı değildir. Etmen tabanlı bir yaklaşımda, başlangıçta, seçmenin elinde sadece oturumu başlatacak küçük bir yazılım parçası olması yeterlidir. Seçmen tarafındaki etmen altyapısı sadece kullanılan oyun başarıyla ulaştığını göstermekle ve oturumu başlatacak ilk iletiyi yetkeye göndermekle görevlidir. Seçmen tarafında da diğer taraflarda olduğu gibi yine yardımcı sınıflar vardır: anahtar yaratmaya yarayan bir sınıf ve zaman ölçen bir sınıf.

Şekil 5.1 Sayman tarafında oylama sonucunun gösterilmesi.

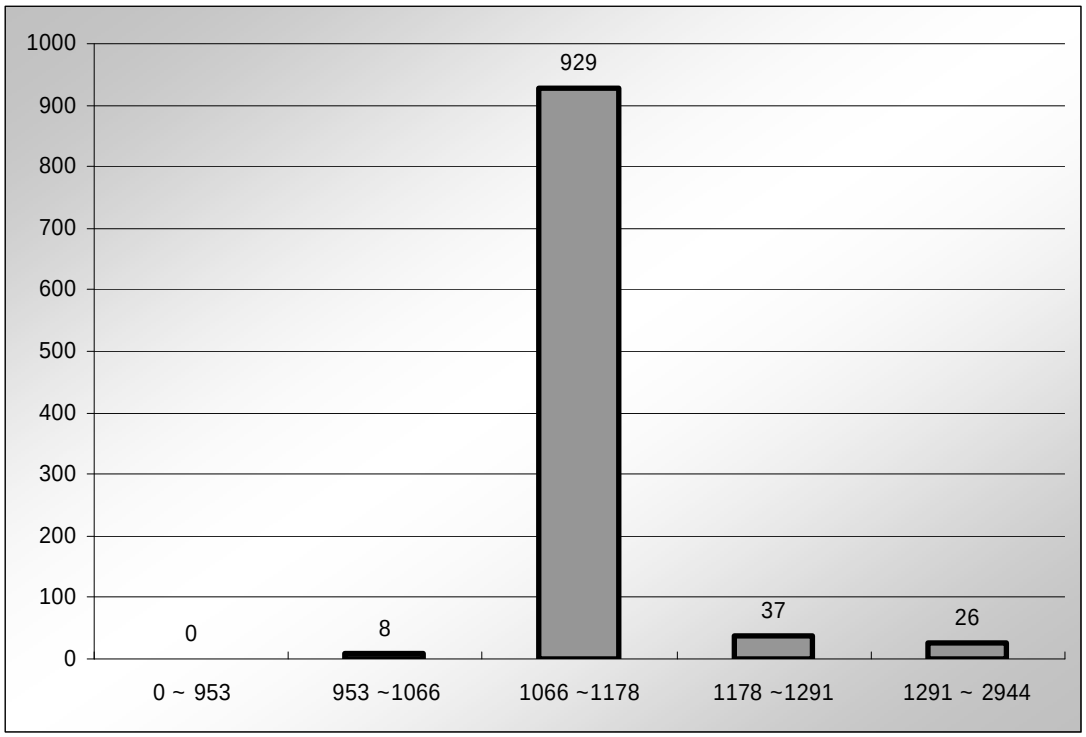
Bu yazılım parçaları kullanılarak konusu bir klasik müzik korosundaki oylama olan bir benzetim yapılarak işlevlerin çalışması ve iletiler izlenmiştir. Benzetim basitçe kurulmuş bir arayüze sahiptir. Ekran fotoğrafları aşağıda bulunan benzetimle önerilen ikinci dizgenin gerçeklenebilir olduğu belirlenmiştir. Sayman tarafında sayım sonucunu gösteren fotoğraf **Şekil 5.1**'de, seçmen tarafından görülen oy pusulası ve başarılı oy kullanıldığını gösteren onay sırasıyla **Şekil 5.2**'de ve **Şekil 5.3**'te gösterilmiştir.

Şekil 5.2 Seçmen tarafında gösterilen oy pusulası.

Şekil 5.3 Seçmene oyun başarıyla kullanıldığını gösteren onay penceresi.

6 OLURLUK

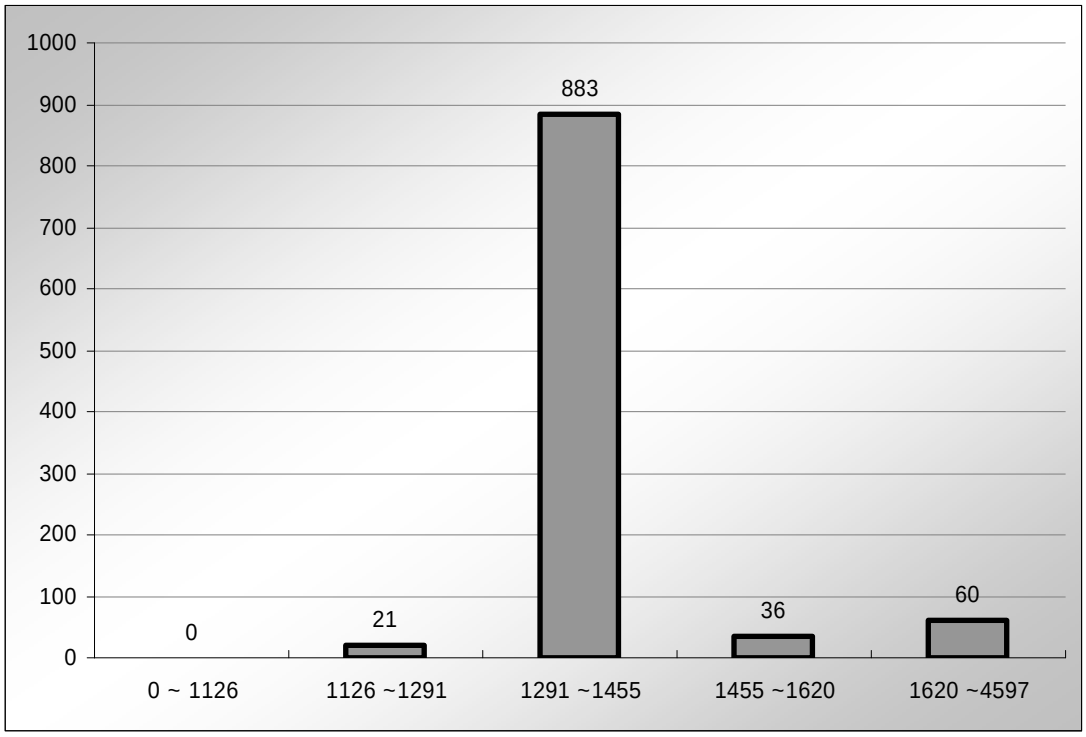
Önerilen ikinci dizgenin benzetimi sırasında 1 yetke, 1 sayman ve 1 ile 1000 arasında seçmen kullanılmıştır. Benzetimde bakışımsız şifreyazım için 1024 ikililik anahtarlara sahip RSA algoritması, bakışımlı şifreyazım için 168 ikililik TripleDES algoritması kullanılmıştır. Benzetim için kullanılan bilgisayar, 1000 MHz işlemci çekirdek hızına ve 512 MB belleğe sahip, Windows 2000 Professional işletim sistemi üzerinde Java2 1.5.04 sanal bilgisayarını çalıştıran sıradan bir kişisel bilgisayardır. Bu giriş değişkenleriyle gerçekleştirilen benzetim sırasında ölçülen değerler kullanılarak olası büyük ölçekli bir oylama için olurluk öngörülebilir.



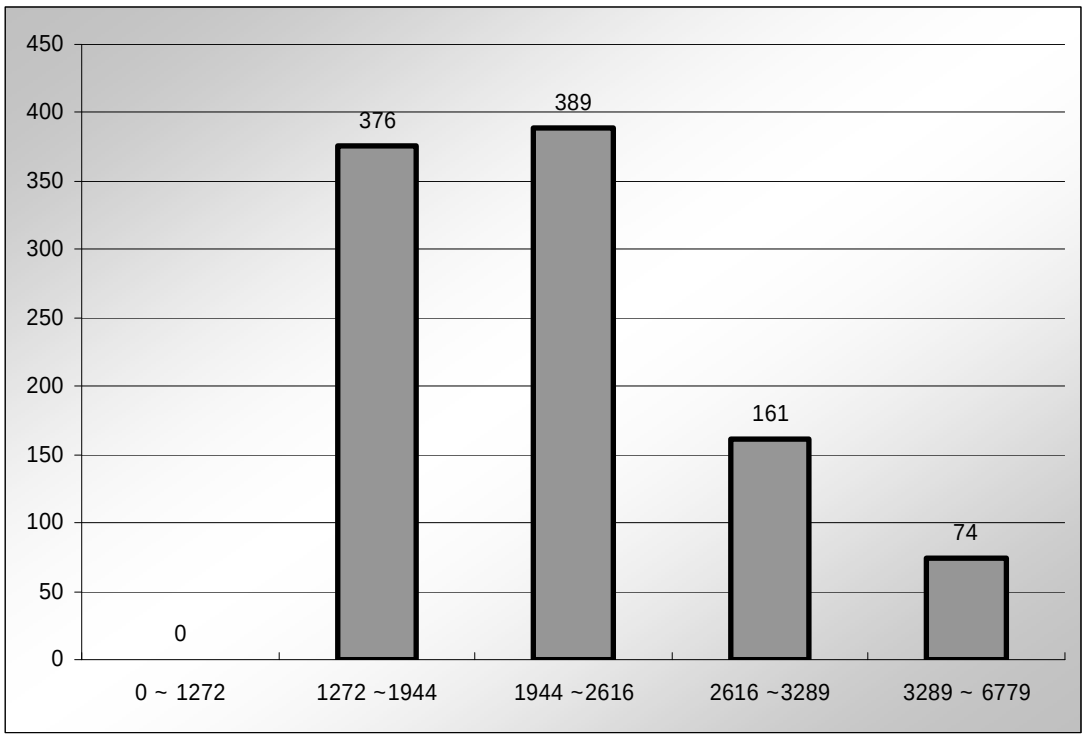
Şekil 6.1 Defter etmeninin oluşturulması için geçen sürelerin histogramı

Benzetim sırasında sözü edilen bilgisayarda 1000 ölçüm yapılmıştır. Buna göre defter etmeninin oluşturulması en az 1061 milisaniye, en çok 2944 milisaniye,

ortalama 1122 milisaniye sürmüştür. Ölçülen değerlere ilişkin histogram **Şekil 6.1**'de gösterilmiştir. Benzer şekilde, pusula etmeninin oluşturulması en az 1272 milisaniye, en çok 4597 milisaniye, ortalama 1373 milisaniye sürmüştür. Ölçülen değerlere ilişkin histogram **Şekil 6.2**'de verilmiştir. Kullanılmış bir oyun sayılması en az 0 milisaniye, en çok 80 milisaniye, ortalama 16 milisaniye sürmüştür. Oyun sayılması için geçen süre ölçülürken ölçüm hatalarının etkisi görülse de, ölçümün ortalama değeri anlamlı görünmektedir. Benzetimde yer alan herhangi bir tarafın bakışımsız anahtar oluşturması için geçen süre en az 1422 milisaniye, en çok 6779 milisaniye, ortalama 2280 milisaniyedir. Ölçülen değerlere ilişkin histogram **Şekil 6.3**'de verilmiştir. Defter etmeninin oluşturulması sırasında yaratılan bakışımlı anahtarın oluşturulması için geçen süre ayrıca ölçülmemiş, defter etmeninin oluşturulma süresi içinde bırakılmıştır. Burada, kullanılmış oy sözüyle belirtilen, rastgele bir sayıya bitişik oy bilgisinin önce yetkenin gizli anahtarıyla ardından da saymanın açık anahtarıyla şifrelenmesiyle oluşturulmuş ve geçerli ve hilesiz yollarla saymana ulaştığı varsayılan metindir. Benzetimde oluşturulan defter etmeninin büyüklüğü 4438 bayt, pusula etmeninin büyüklüğü 5589 bayttır.



Şekil 6.2 Pusula etmeninin oluşturulması için geçen sürelerin histogramı.



Şekil 6.3 Bakışımsız anahtar oluşturulması için geçen sürelerin histogramı.

Bu bilgileri kullanarak defter etmenlerinin oluşturulmasında, taşınmasında ve oyların sayımında harcanacak zamanlar kestirilebilir. Bakışımsız anahtarların oluşturulması için gereken süre kayıt aşamasından önce ya da kayıt aşamasında harcanacağından bu sürenin dizgenin başarımını etkilemeyeceği düşünülebilir.

Defter etmenlerinin oluşturulmasındaki toplam işlem zamanı; 'n_s' seçmen sayısı, 't_d' defter etmenlerinden her birinin [saniye] biriminde hazırlanma süresi olmak üzere, '$Y_d=n_s.t_d$' [saniye] eşitliğiyle hesaplanabilir. Dizgenin çok sayıda aynı özellikte bilgisayarın bir arada çalışması ile gerçekleşeceği ve seçmenlerin bilgisayarlar arasında düzgün dağıldığı düşünülürse her bir bilgisayara düşen işlem zamanı '$y_d=Y_d/n_{by}$' [saniye] eşitliğiyle hesaplanabilir. Bu eşitlikte 'n_{by}', aynı anda çalışacak bilgisayarların sayısıdır.

Pusula etmeni sadece bir kez hazırlanacağından, onun oluşturulması için harcanan zaman önemsenmeyebilir.

Etmenler taşınırken kullanılacak olan bant genişliği etmenlerin büyüklüğü ve sayısıyla hesaplanabilir. Bir seçmenin defter etmenini alması için gereken süre; 'b_s'

her bir seçmenin [ikili/saniye] biriminde sahip olduğu bant genişliği, 's_d' defter etmeninin [bayt] biriminde büyüklüğü olmak üzere, '$t_{td}=8.s_d/b_s$' [saniye] ile belirlenir. Aynı anda çalıştırılan bilgisayarların her birinin sahip olması gereken en düşük bant genişliğini bulmak için birim zamanda bilgisayarlara gelen istek bilinmelidir. Seçmenlerin oylama süresince düzgün aralıklarla başvuru yaptığı düşünüldüğünde birim zamanda gelen istek '$i_d=(n_s.t_{td})/(n_{by}.t_s)$' ile [istek/saniye] biriminde belirlenir. 't_s' [saniye] biriminde oylamanın toplam süresidir. Bu durumda yetkeye ilişkin her bir bilgisayarın sahip olması gereken en düşük bant genişliği '$b_d=8.i_d.s_d$' [ikili/saniye] olacaktır.

Pusula etmeninin saymandan seçmene taşınması için [saniye] biriminde gereken süre; 's_p' pusula etmeninin [bayt] biriminde boyu olmak üzere, benzer şekilde, '$t_{tp}=8.s_p/b_s$' [saniye] ile hesaplanabilir. Pusula etmeni seçmene göre değişmeyeceğinden taşınması sırasında vekil sunuculardan da yararlanılabilir. Bu durumda, pusula etmeninin taşınması için ayrılan bant genişliği önemsenmeyebilir.

Oy verme aşamasında harcanan zaman seçmenlerin bilgisayarında gerçekleştiğinden dizgenin kurulmasında önemli olmadığı düşünülmüş ve burada hasaplanmamıştır.

Sayım aşamasında saymanın her bir oyun şifresini çözmek için harcadığı zaman [saniye] biriminde 't_o', toplam oy sayısı 'n_o', aynı anda çalışan bilgisayar sayısı 'n_{bs}' ile verildiğinde; tüm oyların şifresinin çözülmesi '$t_{şç}=t_o.n_o/n_{bs}$' [saniye] ile belirlenen sürede tamamlanacaktır. Saymanların bir karıştırıcı ağ oluşturacak şekilde yanyana geldiği düşünülürse, karıştırıcı ağın her katmanında bir şifre çözme zamanı harcanacak, sayımın tamamlanması için ise toplam '$T_{şç}=t_{şç}.n_{ka}$' [saniye] süresi gerekecektir. 'n_{ka}', karıştırıcı ağın katmanlarının sayısıdır.

Benzetim sırasında elde edilen değerler kullanılarak bir sanal oylama yaratılabilir ve bazı kestirimler yapılabilir. 8 saat sürecek oylamada, saniyede 56000 ikili bant genişliğine sahip ve hepsi oy kullanan ve oyunu daha sonra değiştirmeyen 10.000.000 seçmen, yetke tarafında eşzamanlı çalışan, yukarıda sözü edilen özelliklere sahip, 10.000 kişisel bilgisayar ve herbir katmanda eşzamanlı çalışan, yukarıda sözü edilen özelliklere sahip, 2.000 kişisel bilgisayarın oluşturduğu 5 katmanlı bir karıştırıcı ağ olduğu düşünülmüştür. Bu durumda defter etmenlerinin oluşturulması denklem (6.1)'de gösterildiği gibi yaklaşık 19 dakika, defter etmeninin seçmene taşınması denklem (6.2)'de gösterildiği gibi yaklaşık 634 milisaniye, pusula etmeninin taşınması denklem (6.3)'te gösterildiği gibi yaklaşık 798 milisaniye, yetke

tarafındaki herbir bilgisayarın sahip olması gereken bant genişliği denklem (6.4)'te gösterildiği gibi saniyede yaklaşık 782 ikili, sayımın tamamlanması denklem (6.5)'te gösterildiği gibi yaklaşık 7 dakika olarak hesaplanacaktır.

$$y_d = \frac{n_s \times t_d}{n_{by}} = \frac{10.000.000 \times 1{,}122}{10.000} = 1122\,sn. \approx 19\,dk. \tag{6.1}$$

$$t_{td} = \frac{8 \times s_d}{b_s} = \frac{8 \times 4438}{56000} \approx 0{,}634\,sn. \tag{6.2}$$

$$t_{tp} = \frac{8 \times s_d}{b_s} = \frac{8 \times 5589}{56000} \approx 0{,}798\,sn. \tag{6.3}$$

$$b_d = 8 \times i_d \times s_d = 8 \times \frac{n_s \times t_{td}}{n_{by} \times t_s} \times s_d = 8 \times \frac{10.000.000 \times 0{,}634}{10.000 \times (8 \times 60 \times 60)} \times 4438 \approx 782\,ikili/sn. \tag{6.4}$$

$$T_{şç} = \frac{t_o \times n_o}{n_{bs}} \times n_{ka} = \frac{0{,}016 \times 10.000.000}{2.000} \times 5 = 400\,sn. \approx 7\,dk. \tag{6.5}$$

Elde edilen değerler kabul edilebilir görünse de, bu kestirimler sırasında bir çok idealleştirme yapıldığı unutulmamalıdır. Etmenlerin taşınması dışında kalan iletişimde harcanan kaynaklar, oy değiştirmeler sırasında harcanan kaynaklar, sunucuların gelen iletileri yorumlaması sırasında harcanan kaynaklar ve veri tabanı sorgulamaları sırasında harcanan kaynaklar benzetim sonuçlarına bakarak kestirilmesi zor harcamalardır; bu nedenle, yukarıda görülen değerler bu harcamalar yok sayılarak hesaplanmıştır.

Bunun yanında, hem gereken en düşün bant genişliği hem de işlem süreleri, üzerlerine büyük oranda hata payı eklense bile uygulanabilir görünmektedir. Özellikle yetke tarafındaki sunucular başına düşen oldukça düşük bant genişliği gözlendiğinde, her bir sunucunun gerekli veritabanı sorgulamalarına da, iletileri işlemeye de yeterince zamanı kalacağı düşünülebilir. Ters bir bakış açısıyla, yetke

tarafında kullanılan bilgisayar sayısı azaltılarak dizgenin ucuzlatılması da denenebilir. Geçmiş oylamalarda gerçekleşmiş gerçek seçmen davranışlarına ilişkin istatistiklere erişilebilirse, bunların incelenmesiyle hem zaman hem de değer açısından en iyileştirilmiş bir dizge oluşturulması bu aşamada olanaklı görünmektedir.

7 SONUÇ

Çalışmada; elektronik oylama, etmen tabanlı yaklaşım, temel şifreyazım yöntemleri ve çalışmada kullanılan özel şifreyazım yöntemleri, genel bir oylamanın sağlaması gereken koşullar ve bunların sağlanmasında bugüne dek karşılaşılmış zorluklar anlatılmıştır. Bir oylamanın sağlaması gereken koşullar belirlenirken daha önce yayınlanmış çalışmalar içinde derin bir araştırma yapılmış, çalışmayla ilgili olanlar ve olmayanlar sınıflandırılmış, kavramsal olarak farklı görünse de teknik açıdan birbiriyle örtüşen koşullar bir araya getirilmiştir. Koşulların sağlanmasında bugüne dek raporlanmış sorunlar ve olabileceği kestirilen sorunlardan söz edilmiştir. Çalışmanın amacı, gerekli koşulları sağlayan ayrıca sözü edilen sorunların oluşumuna elden geldiğince olanak vermeyen bir oylama dizgesinin oluşturulmasıdır. Tasarım sırasında görülen sorunlara çözümler aranırken farklı yaklaşımlarla tasarım iki ayrı yola sürüklenmiş, sonunda kendi içlerinde tutarlı iki ayrı tasarım ortaya çıkmıştır.

Yaklaşık yirmi yıldır sürdürülen elektronik oylama çalışmalarının tarihi bir özet biçeminde çalışmada yer almaktadır. Bugüne dek yapılan çalışmalar uzun süre araştırılmış, olasılıkla yayınlanmış her görüşe ulaşılmış, ulaşılabilen çalışmalar incelenmiş, eksikleri ve yararları belirtilmiştir.

Yeni elektronik oylama yöntemleri önerilirken kendisinin güvenliği –çalışmada görülebileceği gibi çözülmesi olanaklı olan– ayrı bir sorun yaratsa da, dizgenin pek çok güvenlik sorununun çözülmesine yardımcı olan etmen tabanlı yaklaşım seçilmiştir. Oluşturulan yöntemler; tanımları, işleyişleri, güvenlikleri üzerinde tartışılarak açıklanmış; var olan dizgelerle karşılaştırılmışlardır.

Yöntemler arasından birincisini kapsayıcı olan ikincisi seçilerek bir benzetim yapılmıştır. İkinci yöntemin benzetiminin gerçekleştirilmesiyle, birincisinin de gerçekleştirilebileceği söylenebilir. Önerilen yöntemin uygulanabilirliğini gösteren benzetim sırasında dizgenin olurluğunu kestirmeye yönelik ölçümler de yapılmıştır.

Dizgenin oluşturulmasının ardından, büyük ölçekte kullanılabilir olup olmadığının kestirilebilmesi için önerilen denklemler doğrultusunda yapılan hesaplar, dizgenin büyük harcamalara gerek duyulmaksızın her ölçekte kullanılabileceğini göstermektedir.

Yöntemlerin üstün yanlarına yapılan göndermeleri gelecekte uygulanabileceği olası alanlarla ilgili öngörüleri ve yöntemin ilerletilmesine ve iyileştirilmesine yönelik taze düşünceleri içeren bu sonuç bölümüyle çalışma tamamlanacaktır.

Önerilen yöntemlerin olasılıkla en önemli getirisi sunucuları gerçek zamanda hesap yapmaktan kurtarmasıdır. Oldukça ağır olan şifrebilimsel hesapları yapmak zorunda kalmayacak sunucuların sığaları ciddi anlamda düşürülebilir, böylece oldukça ucuz elektronik oylama dizgeleri oluşturulabilir.

Önerilen yöntemlerde etmenlerin kullanılması dizgenin kötü niyetli kişilerce bozulmasını engelleyecektir. Oy verme aşamasında kullanılan etmenler seçmenlerin olası etkilerini sınırlayarak seçmenleri yönlendirebilir, aynı biçimde davranmalarını sağlayabilir. Bunun yanında dizgede yapılması gerekli görülen bir değişiklik ya da güncelleme için geniş çaplı bir çalışma gerekmez. Oylamanın başlayacağı ana kadar değiştirilebilir bir dizge oluşturulabilir.

Etmenler yapıları gereği bir çok değişik ortamda, değişik altyapılarda, değişik mimarîlerde ya da değişik işletim sistemlerinde çalışabilirler. Uygun etmen ve konak tasarımlarıyla dizge sadece bilgisayarları ya da benzer bir elektronik araçlar kümesini kullanarak değil, iletişim kurabilen her aracı kullanarak geliştirilebilir. Bu önerilen dizgenin günümüzde yaygın kullanılan GSM şebekelerinde de kullanılabilecek bir dizgeye dönüştürülebileceği anlamına gelir. Bu dönüşüm, aynı zamanda, asıllama sırasında kullanılması önerilen akıllı kartların zaten var olduğu bir ortam kullanılacağından dizgenin hayata geçirilmesindeki toplam harcamayı da azaltacaktır.

Alışıldık, bilinen ve güvenilirliği uzun yıllardır denenmiş şifrebilimsel yöntemler dışında yeni bir yöntem kullanmadan, etmen yaklaşımını daha önce uygulanmış oylama yöntemleriyle birleştirerek oluşturulan bu yeni yaklaşımla gerçek zamanda hesap gereğini ortadan kaldıran, özelleştirilebilir, uzaktan denetlenebilir, esnek, güvenilir ve en önemlisi ucuz bir dizge oluşturulmuştur.

Önerilen yöntemlerin yanına eklenebilecek yine etmen tabanlı üçüncü bir yöntemin daha verimli bir dizge oluşturabileceği düşünülmüştür. Körleştirme tabanlı bir yaklaşım yerine eşişlem tabanlı bir yaklaşımla etmenlere uygulanacak bir dizge başarılı olabilir. Eşişlemli şifreyazım ile bir seçmen kümesinin oyları seçmenlerin kimliğinden bağımsız biçimde, kavramsal olarak alışıldık oylama dizgelerindeki oy sandığının yerine geçen bir etmen aracılığıyla toplanabilir.

Önerilen dizgenin ya da bu temelde geliştirilecek yeni dizgelerin yaygın olarak kullanılmasıyla gerçekte konumuz içinde olmasa da sosyal ve politik bilimler tarafından sıkça vurgulanan karar sürecine katılım sorununa, yani temsili demokrasi yönetiminin günümüzdeki –olasılıkla en ciddi– sorununa, etkin bir çözüm getirilebilecek ve seçmenlerin katılımı büyük olasılıkla artırılacaktır.

KAYNAKLAR

[1] **Ku, Ho**, 2004. An e-Voting Scheme against Bribe and Coercion, *Prooceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service*, Taipei, Tayvan, 28-31 Mart.

[2] **S. Goldwasser, S. Micali and C. Rackoff**, 1989. The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, **18**, 186–208.

[3] **A. Kiayias, M. Yung**, 2004. The Vector-Ballot E-Voting Approach, *Financial Cryptography 2004*, Key West, Florida, ABD, 9-12 Şubat.

[4] **W. A. Arbaugh, 2004**. The Real Risk of Digital Voting?, *Computer*, Aralık, s. 124–125.

[5] **Internet Policy Institute**, 2001. *Report of the National Workshop on Internet Voting: Issues and Research Agenda*, Maryland, ABD.

[6] **M. Stadler, J.M. Piveteau, and J. Carmenisch**, 1995. Fair blind signatures, *Advances in Cryptology - Eurocrypt '95*, St.Malo, Fransa, 21-25 Mayıs, s. 209–219.

[7] **Benaloh**, 1996. Verifiable Secret-Ballot Elections, *Doktora Tezi*, Yale University, New Haven, ABD.

[8] **D. Chaum**, 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, *Communications of the ACM*, **24(2)**, 84–88

[9] **M. Abe, F. Hoshino**, 2001. Remarks on Mix-Networks Based on Permutation Networks, *PKC 2001*, Cheju Island, Kore, 13-15 Şubat.

[10] **D. Boneh, P. Golle**, 2002. Almost Entirely Correct Mixing With Applications to Voting, *9th ACM-CCS Conference*, Washington, ABD, 17-21 Kasım.

[11] **J. Furukawa, K. Sako**, 2001. An Efficient Scheme for Proving a Shuffle, *CRYPTO 2001*, Santa Barbara, ABD, 19-23 Ağustos.

[12] **P. Golle et al.**, 2002. Optimistic mixing for Exit-Polls, *Asiacrypt 2002*, Queenstown, Yeni Zelanda, 1-5 Aralık.

[13] **M. Jakobsson, A. Juels, R.L. Rivest**, 2002. Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking, *USENIX Security Symposium*, San Francisco, ABD, 5-9 Ağustos.

[14] **D. Chaum**, 2004. Secret-Ballot Receipts: True Voter-Verifiable Elections, *IEEE Security & Privacy*, Nisan, s. 37–47.

[15] **O. Baudron et al.**, 2001. Practical Multi-Candidate Election System, *PODC 2001*, Rhode Island, ABD, 26-29 Ağustos.

[16] **R. Cramer et al.**, 1997. A Secure and Optimally Efficient Multi-Authority Election Scheme, *Eurocrypt 1997*, Konstanz, Almanya, 11-15 Mayıs.

[17] **P. Fouque et al.**, 2000. Sharing Decryption in the Context of Voting or Lotteries, *Financial Cryptography 2000*, Anguilla, British West Indies, 21-24 Şubat.

[18] **B. Schoenmakers**, 1999. A Simple Publicly Verifiable Secret Sharing Scheme and its Applications to Electronic Voting, *Crypto 1999*, Santa Barbara, ABD, 15-19 Ağustos.

[19] **G. Dini**, 2002. A Secure and available electronic voting service for a large-scale distributed system, *Future Generation Computer Systems*, **19**, s. 69–85.

[20] **C.-C. Chang, W.-B. Wu**, 1997. A secure voting system on a public network, *Networks*, **29 (2)**, 81–87.

[21] **D. Chaum**, 1988. Elections with unconditionally secrets ballots and disruption equivalent to breaking RSA, *Proceedings of Eurocrypt'88*, Davos, İsviçre, 25-27 Mayıs, s. 177–182.

[22] **J.D. Cohen, M.J. Fischer**, 1985. A robust and verifiable cryptographically secure election schema, *Proceedings of the 26th IEEE Annual Symposium on Foundations of Computer Science*, Kasım, s. 372–382.

[23] **K.R. Iverson**, 1991. A cryptographic schema for computerized general elections, *Proceeding of Advances in Cryptology— CRYPTO'91*, Santa Barbara, ABD, 11–15 Ağustos, s. 405–419.

[24] **H. Nurmi, A. Salomaa, L. Santean**, 1991. Secret ballot elections in computer networks, *Computer Security*, **10 (6)**, s. 553–560.

[25] **J. Karro, J. Wang**, Towards a practical, secure, and very large scale online election, *Proceedings of the 15th IEEE Annual Computer Security Applications Conference*, Phoenix, ABD, 6-10 Aralık, s. 161–169.

[26] **R.S.-N.A. Baraani-Dastjerdi, J. Pieprzyk**, 1995. Secure voting protocol using threshold schemas, *Proceedings of the 11th IEEE Annual Computer Security Applications Conference*, New Orleans, ABD, Aralık, s. 143–148.

[27] **C. Boyd**, 1989. A new multiple keys cipher and an improved voting schema, *Proceedings of Advances in Cryptology—EUROCRYPT'89*, Hounthalen, Belçika, 10-13 Nisan. s. 617–625.

[28] **D. Malkhi, M.K. Reiter**, 1998. Byzantine quorum systems, *Distributed Computing*, **11 (4)**, s.203–213.

[29] **F. Hohl**, 1998. Time Limited Blackbox Security Protecting Mobile Agents From Malicious Hosts, *Lecture Notes in Computer Science*, **1419**, s. 92–113.

[30] **A. Wagner**, 2005. Implementing Mobile Agent Security in an Untrusting Computing Environment, *Proceedings of the 8th International Conference on Telecommunication*, Zagreb, Hırvatistan, Haziran, s. 591–594.

ÖZGEÇMİŞ

Mehmet Tahir SANDIKKAYA 25 Şubat 1979 tarihinde, Ankara'da, esnaf bir baba ile ev hanımı bir annenin dördüncü çocuğu olarak doğdu. Ankara İltekin İlkokulu'nu bitirdikten sonra 1990 yılında Ankara Atatürk Anadolu Lisesi'ni kazandı. 1998 yılında kabul edildiği İstanbul Teknik Üniversitesi'nde öğrenimini sürdürmek üzere İstanbul'a taşındı. Öğrenimi süresince aralarında ASELSAN A.Ş. ve IBM'in de bulunduğu birçok özel şirketin bilgisayar ve elektronik bölümlerinde ve İstanbul Teknik Üniversitesi bünyesinde çalıştı. 2002 yılında İstanbul Teknik Üniversitesi Elektrik Mühendisliği Bölümü'nü tamamlayıp, İstanbul Teknik Üniversitesi'ne bağlı Bilişim Enstitüsü'nün Bilgisayar Bilimleri Programı'nda yüksek lisans öğrenimine başladı. Aynı yıl, aynı kurumda başladığı görevini Araştırma Görevlisi ünvanıyla sürdürmektedir. Uluslararası SELIT 2001 ve APIS 2004, ulusal ABG 2005 konferanslarına katılmış, uluslararsı 6. ESSE konferansında bir bildiri sunmuştur. Uluslararsı IEEE örgütünün bir üyesi ve örgütün Güç Mühendisliği Topluluğu'nun Türkiye'deki Öğrenci Kolu'nun başkanıdır. Amatör olarak tiyatro, sinema, fotoğraf, astronomi, takı ve müzik ile ilgilenmektedir.