BÖLÜM 10

TEST YÖNTEMLERİ

Giriş

Rassallığın tanımı kısaca tahmin edilemeyen, belirli bir kalıba sahip olmayan olarak verilebilir. Rassal olarak üretilen sayılar, şans oyunlarında, istatistiksel örneklemelerde ve simulasyon uygulamalarında sıkça kullanılır.

Rassallık kriptografide kullanılan en temel özelliklerden biridir. Atak yapan kişiye, bir kriptosistem çıktısının olabildiğince tahmin edilemez olması gerekir. Rassal sayılar birçok kriptografik uygulamanın temelini oluşturur. Oluşturulması en gerekli ve aynı zamanda en zor olan kısımdır. Neredeyse bütün kriptografik protokollerde gizli ve tahmin edilmesi zor değerlere ihtiyaç duyulur, örneğin asimetrik şifreleme yöntemlerinde (RSA, Diffie Hellman) anahtar oluşturulurken, rassal sayılar kullanılır. Anahtar gizliliği kriptosistemlerde çok önemli olduğu için, programlama dillerinde standart olarak kullanılan rassal sayı üreteçlerinin kriptografik amaçlar için kullanılması sakıncalıdır. Genelde, bu algoritmalar istatistiksel rassallık için tasarlanmıştır, kriptanalize karşı dayanıklı değillerdir). Temel olarak rassal sayılar iki farklı yöntemle oluşturulur:

Gerçek rassal sayı üreteçleri içinde rassal bir yapı bulunduran fiziksel sinyal kaynakları kullanarak dizi üretirler. Bu üreteçlerin en önemli avantajları:

- Dizinin bir kısmına sahipken, farklı bir kısmını elde etmenin mümkün olmaması;

- Üretilen diziler kendi içinde herhangi bir gizli bağıntının bulunmaması;
- Periyodik olmamalarıdır.

Bu avantajların yanı sıra, gerçek rassal sayı üreteçlerinin önemli dezavantajları da bulunur. Bu üreteçler çoğunlukla verimsizdir, uzun sayı dizileri elde etmenin maliyeti yüksektir. Deneyi tekrarlayıp bir sayı dizisini yeniden elde etmek mümkün değildir.

Sözde-rassal (pseudo-random) sayı üreteçleri matematiksel algoritmalar kullanarak diziler üretirler. Bu algoritmalar kendi içlerinde herhangi bir rassallık barındırmazlar, algoritmalar da genelde açıktır. Buradaki rassallık algoritmaların girdileri (seed) ile sağlanır, bu yüzden algoritmaların girdileri gizli tutulmalıdır ve kolay tahmin edilemez olmalıdır. Algoritma ve girdi bilinirse, dizinin tümü elde edilebilir. Bu üreteçler verimlidir ve uzun diziler üretmenin maliyet düşüktür. Kriptografik olarak kullanılabilecek sözde-rassal sayı üreteçleri ile üretilen bir dizinin bir kısmı biliniyorsa, bu dizinin diğer kısımları ile ilgili bir bilgi vermemelidir. Aynı üreteçle üretilen farklı diziler birbirleri ile ilişkileri olmamadılır (correlation). Dizilerin periyotları mümkün olduğunca uzun olmalıdır.

$0-1$ Dizileri

Kritografide kullanılan sayı dizileri 0 ve 1'lerden oluşur. Sayı üretecinin ürettiği her bitin 0 veya 1 olma ihtimali $\frac{1}{2}$ye eşit olmalıdır. Golumb, periyodik bir dizinin rassallığını test eden üç tane kural geliştirmiştir:

1. Dizi içerinse bulunan 0'ların ve 1'lerin sayısının farkı maksimum 1 olmalı.

2. Dizi içerisinde bulunan öbeklerin (kendisini tekrarlayan bitler) sayısı, n dizi uzunluğu olarak verildiğinde, $(n+1)/2$ olmalıdır. Bir bitten oluşan öbeklerin sayısı toplam öbek sayısının yarısı kadar olmalıdır.

3. Dizinin kendisi ile olan ilişkisi düşük olmalıdır.

Bir dizinin rassallığı test edilirken Golumb kuralları yeterli değildir. LFSR'lar ile üretilen sayı dizileri Golumb kurallarını sağlamalarına rağmen kriptografik olarak sayı üreteçleri olarak kullanılmazlar. LFSR ile üretilen sayı dizilerinin lineer karmaşıklıkları düşüktür.

Sözde-Rassal Sayı Üreteçlerinin Test Edilmesi

Sözde-rassal sayı üreteçlerini test etmek için istatistiksel testler kullanılır. Aşağıda istatistiksel hipotez testleri ile ilgili önbilgi bulunmaktadır.

İstatistiksel Testler

İstatistiksel çıkarım yapmak için istatistiksel hipotez testleri kullanılır. Bu testlerde bir hipotez (null hypothesis, H_0) öne sürülür, bu hipotezin tersi de alternatif hipotez, Ha olarak kabul edilir. İstatistiksel test sonucunda varılabilecek iki farklı temel karar vardır: - H_0' yu reddet. - H_0' yu reddetme. Birinci karar, H_0 aleyhine güçlü bir kanıt elde edildiğinde verilir. Bu güçlü kanıt bulunamadığında ise ikinci karar verilir.

Bütün istatistiksel testlerde kaçınılmaz hata yapma payı vardır. Test sonucunda iki farklı hata, birinci tip (alfa) ve ikinci tip (beta) yapılabilir. Birinci tip hata hipotezimiz doğruyken, kararımız H_0'yu reddet olduğunda gerçekleşir. İkinci tip hata ise hipotezimiz yanlışken, kararımız H_0'yu reddetme olduğunda gerçekleşir. Hipotez testinde birinci

tip hata yapma olasılığını sınırlamak gerekir. Test sonucunda birinci tip hata yapma olasılığımız, testimizin güvenilirlik seviyesini verir. Bu değer genel olarak 0.01-0.05 olarak seçilir. İstatistiksel bir testin gücü, ikinci tip hatayı yapmama olasılığına eşittir. Testin gücünü arttırmak için daha fazla örnekleme yapılır.

İstatistiksel bir test yapılacağında ilk olarak, H_0 ve H_a belirlenir. Daha sonra testin güvenilirlik seviyesine karar verilir. Bir örnekleme yapılır ve test istatistiği ve buna bağlı olarak p-değeri hesaplanır. P-değeri, birinci tip hata yapma olasılığını kontrol etmek yerine, H_0'ın doğru olduğu varsayımı ile test istatistiğinin gözlemleme değeri veya daha uç bir değer olması olasılığına karşılık gelir. Bu tanıma uygun olarak hesaplanan olasılık p-değerini verir. Eğer bu değer seçilen güvenilirlik değerinden küçükse H_0 hipotezi reddedilir.

İstatistiksel testlerde en çok kullanılan dağılımlar Normal ve Ki-kare dağılımlarıdır.

Normal Dağılım

Gauss Dağılımı adı ile de bilinen normal dağılım ilk kez De Moivre tarafından bulunmuştur. Genelde, hipotez testleri dağılımın normal olduğu varsayımına göre düzenlenir. Dağılımın ortalama ve standart sapma olmak üzere iki parametresi vardır. Çan eğrisi olarak da bilinir. Eğrinin tepe noktası ortalamasına denk gelir. Ayrıca bu dağılımda ortalama, medyan ve mod aynı değerdir. Ortalamaya göre simetrik bir grafiği vardır. Dağılımın standart sapması eğrinin genişliğini belirler.

Ortalaması sıfır ve standart sapması 1 olan normal dağılıma sahip bir değişkenin dağılımına standart normal dağılım denir. Standart normal dağılıma sahip değişkenler

Z ile gösterilir.

Ortalamadan iki yöne 1,2 ve 3 standart sapma kadar uzaklaşıldığında, toplam alanın sırasıyla %68.26 , %95.44 ve %99.74'ü kapsanır.

Ki-Kare Dağılımı

Standart normal bir dağılımdan seçilen bir birimin x değerinin karesi bir ki-kare değeri olur. Bu şekilde tek bir birimden elde edilen ki-karelerin dağılımı bir serbestlik derecelidir. Standart normal bir dağılımdan seçilen n değerin karelerinin toplamı n serbestlik dereceli bir ki-kare dağılımı olur. Dağılımın şekli serbestlik derecesine göre değişir ve asimetriktir. Sürekli bir dağılıma sahiptir.

NIST Test Paketi

Sayı üreteçlerinin rassallığını ölçmek için bir istatistiksel test yeterli değildir. Bu konuda birçok test paketi üretilmiştir (FIBS 140 - Queensland University, DieHard - Florida State University, NIST). NIST paketinden seçilen bazı testlerin açıklaması aşağıda verilmiştir. NIST paketindeki testler ile ilgili daha ayrıntılı bilgi için : http://csrc.nist.gov/rng/

Frekans Testi

Verilen bir dizide bulunan 0 ve 1'lerin oranını kontrol eder. Testin herhangi bir parametresi yoktur. Testte kullanılan referans dağılım yarım normal dağılımdır. Testin sonunda elde edilen p-değeri çok küçük çıkması, dizideki 1'lerin yada 0'ların sayısının beklenenden fazla olduğunu gösterir. Testin geçerli olabilmesi için dizi uzunluğunun enaz 100 olması gerekir.

Blok Frekans Testi

Verilen bir dizide bulunan 0 ve 1'lerin oranını M bitlik bloklar içinde kontrol eder. Testin tek parametresi blok uzunluğudur (M). Blok uzunluğu 1 olarak alındığında blok frekans testi, frekans testine dönüşür. Herbir bloktaki 1'lerin beklenen oranı $M/2$'dir. Testte kullanılan referans dağılım ki-kare dağılımdır. Testin sonunda elde edilen p-değeri çok küçük çıkması, dizideki bloklarda 1'lerin ve 0'ların oranının $\frac{1}{1}$'den fazlasıyla saptığını gösterir. Testin geçerli olabilmesi için blok uzunluğunun en az 20, dizi uzunluğunun da en az 100 olması gerekir.

Öbek Testi

Dizide bulunan öbeklerin (birbirlerini tekrarlayan bitlerin) sayısını kontrol eder. Test, frekans testinden geçmiş dizilere uygulanır. Dizideki değişimler ne çok hızlı (örn. 01010101), ne de çok yavaş (örn. 00001111) olmalıdır. Testte kullanılan referans dağılım ki-kare dağılımdır. Testin geçerli olabilmesi için dizi uzunluğunun en az 100 olması gerekir.

Bloktaki En Uzun Birler Testi

Test, M-bitlik bloklarda bulunan en uzun birler grubu üzerinde odaklaşır. Testin tek parametresi blok uzunluğudur (M). Dizi M-bitlik n tane bloğa bölünür ve her blok içerisindeki en uzun birler öbeğinin uzunluğuna bakılır. Bu değerlerin frekansları beklenen değerlerle kıyaslanır ve ciddi bir sapma olup olmadığı kontrol edilir. Testte kullanılan referans dağılım ki-kare dağılımdır. Dizi uzunluğuna göre blok uzunluğu ve blok sayısına karar verilir.

Matris Rank Testi

Test içerisinde dizi $M * M$-bitlik matrislere bölünür ve oluşturulan herbir matrisin rankı hesaplanır. Diziden oluşturulan matrislerin ranklarının frekansları hesaplanır, beklenen frekansla kıyaslanır ve ciddi bir sapma olup olmadığı kontrol edilir. Testte kullanılan referans dağılım ki-kare dağılımdır. Dizi uzunluğuna göre matrisin boyutlarına karar verilir. Önerilen $M = 32$ değeri için dizi uzunluğu en az 38,912 bit olmalıdır.

Evrensel Test

Verilen dizinin yeterince sıkıştırılıp sıkıştırılamayacağını kontrol eder. Dizinin fazlasıyla sıkıştırılması, dizinin rassallıktan uzak olduğunu gösterir. Testte, dizi L bitlik bloklara ayrılır. Bu blokların bir kısmı testin başlangıç kısmında uygulanır. Testte kullanılan referans dağılım yarım normal dağılımdır. L-bitlik kalıpların birbirlerini ne kadar sıklıkla tekrar ettiği hesaplanır ve bu değerler beklenen değerler ile karşılaştırılır. Blok uzunluğu 6 seçildiğinde, dizi uzunluğu en az 387,840 olmalıdır.

Lineer Karmaşıklık Testi

Test dizinin rassallık için yeterince karmaşık olup olmadığını kontrol eder. Diziler LFSR çıktıları olarak kabul edilir ve diziyi oluşturabilecek en küçük LFSR'ın boyu küçükse, dizinin rassal olmak için yeterince karmaşık olmadığına karar verilir. Testte dizi M bitlik bloklara ayrılır ve bloktaki bitlerin lineer karmaşıklıkları Berlekamp-Massey algoritması kullanılarak hesaplanır. Hesaplanan lineer karmaşıklıkların beklenen dağılıma uygun olup olmadıklarına bakılır. Testte kullanılan referans dağılım ki-kare dağılımıdır. Testin geçerli olabilmesi için dizinin boyu en az 1,000,000; blok uzunluğu da 500 ve 5000 arasında olmalıdır.

Entropi Testi

Test, m bitlik kesişen blokların frekansları üzerinde odaklaşır ve bu frekansları m ve $(m+1)$-bitlik bloklar için beklenen değerler ile karşılaştırır. Testte kullanılan referans dağılım ki-kare dağılımıdır. Diziden kesişen n tane m-bitlik blok üretilir. Bu blokların frekansları ve entropisi hesaplanır. Aynı işlemler blok uzunluğu $m+14$ için tekrarlanır. m ve $m+1$ bit için hesaplanan değerlerin farkına bağlı test istatistiği hesaplanır. Bu farkın düşük olması rassallıktan uzaklığı gösterir.

Değerlendirme Stratejileri

Verilen rassal sayı üreteci kullanılarak uzunluğu n olan m adet sayı dizisi oluşturulur. Bu m dizi verilen testlere girdi olarak kullanılır. Testlerin sonucunda $m*$(test sayısı) kadar p-değeri hesaplanır. Bu p-değerlerinin analizi sonucunda üretecin sağladığı rassallık hakkında karara varılır. Burada 3 farklı karar verilebilir; (1) Rassallıktan sapma belirlenmedi, (2) Açıkca rassallıktan sapma belirlendi, (3) Belirli bir sonuca varılmadı. Bu kararlar verilirken öncelikle testin güvenilirlik seviyesinden düşük kaç tane p değeri bulunduğu ölçülür, bunun beklenen değeri $m*$(test sayısı)$*$(güvenilirlik seviyesi)'dir. Buna ek olarak bulunan üretecin kabul edilmesi için p-değerlerinin dağılımının da tek düze (uniform) olması beklenir.