Klasik Bilgisayar Mantığıyla

Şifreli Kuantum İletişim Protokolü

Mesut Kavak[*a*]

Bir süredir evreni yöneten temel kanunlar üzerine çalışıyorum. Görünen o ki; herhangi bir fiziksel olguya neden olan en temel ve etkileyici ilke; Heisenberg'in Belirsizlik İlkesi, varlığın herhangi bir özelliğinin belirsizlik nedeniyle var olduğudur.

Bu süreçte bilginin korunması üzerine düşünürken şunu fark ettim ki; bilgi, asla kaybolamaz; ama bir noktada alternatifi olmadığı için bize göre tamamen tanınmaz hale geliyor. Her türlü bilgi ve aranan bilgi bize göre bir noktadan sonra aynı hale geliyor. Duyarlılık sonsuza kadar artar ama kaybolmaz. Her hassasiyet seviyesi ayrıca daha yüksek seviyeye sahiptir; ki yani aslında mutlak bir koruma mümkün görünüyor.

"Peki böyle bir koruma, donanımsal olmayan bir kuantum sistem dışında da örneğin kuantum tünelleme ile öngürülemez olarak bilgi korunumunu amaçlayan bir kuantum etkisi yakalayarak mümkün müdür?"

[*a*]kavakmesut@outlook.com.tr

I. Giriş

Teori *"Belirsizliğe uygun olarak, maddenin ölçülebilir herhangi bir fiziksel değeri mutlaklık ile mutlak yokluk arasında artar veya azalır; fakat asla kaybolmaz. Hiçbir fiziksel değer belirli bir değer alamaz. Sadece bazı yaklaşımlar olarak ifade edilebilirler."*

Bu durumun bir sonucu olarak, örneğin, bir CPU'nun işlem numarasını ölçmek istiyorsanız, her ölçümde en azından virgülden sonraki sayılar için hassaslaştıkça ölçüm işlemi ya da aynı hassasiyetle farklı tekrarlar sonucunda yalnızca bazı farklı sayılar elde edebilirsiniz.

Daha hassas ölçmek istediğinizde virgülden sonra sabit rakamlardan sonra yeni farklı rakamlar çıkar. Bunun dışında asla belli bir sayı elde edemezsiniz.

Ayrıca yine örneğin bir bölme ya da çarpma işlemi yaparsanız aynı işlem için işlemci her zaman işlemi farklı zamanlarda gerçekleştirir. Evet, 32 veya 64 gibi bazı paketlerle performans gösterir ve size her zaman aynı sayıyı verir ki aslında bu da kesin değildir, her tekrar için aynı anda performans göstermez. Bunu öğrenmek için aralığı ayarlarsanız ve bunu bir program üzerinden sorarsanız, bazen 1 saniyede 50'de 1 veya 20'de 1 gibi öngörülemeyen değişen sıklıklarla 33 veya 65 gibi sonuçlar alabilirsiniz.

Aslında bu fiziksel ilke ve koşul, mükemmel bir öngörülemez siber uzay güvenlik unsuru olarak kullanılabilir; çünkü aşağıdaki gibi hesaplanamayan ve öngörülemeyen kodları seçmenin bir yolunu oluşturur.

II. Öngörülemez Seçim

Ondalık sayıları en yakın olana yuvarlayarak kullanalım. Örneğin bir sayı x,xxxx6 ise x,xxxxx'e yuvarlanır ve bu koşul 1 olarak adlandırılır. Sayı x,xxxx4 gibi ise x,xxxx'e yuvarlanır ve koşul 0 olarak adlandırılır. Sayı x,xxxx5 gibiyse tekrar deneyin. Bu 0 ve 1 bit değildir.

Ayrıca bu ikincisini kullandığım diğer birçok yoldan başka bir yol daha var. Örneğin, bir zamanlayıcı geri sayım yaparken, bir sayıya kadar sayma zamanını sorun. Geri sayımı tekrar tekrar yaparsanız, birçok kez aynı sayıyı alırsınız, ancak bazen gerçek sayıya en yakın olan farklı bir sayı alırsınız. Aşağıdaki VB kodları bunun içindir.

Not Sadece 3 metin kutusu, 2 zamanlayıcı ve 1 düğme kullanın ve ardından aşağıdaki kodu kopyalayın. 1000'den 998'e kadar 1'e kadar sayar. Textbox3.Text 10'a kadar 3 olarak ayarlanır.

- Değerleri değiştirebilirsiniz; fakat bu yukarıdaki değerlerin üzerinde Textbox3.Text birçok kez 1 olurken aynı tuş ile aynı işlemi tekrarladığınızda bazen 2 olur.
- Tekrarlar için aynı buton üzerinden istediğiniz frekansı kullanabilirsiniz. Emin olmak için özellikle uzun aralıklı tıklamalar kullanın. Ayrıca otomatik tekrar programı oluşturabilirsiniz.

Single Counter.exe adlı aşağıdaki programı aşağıdaki adresten indirebilirsiniz:

- `https://zenodo.org/record/1450385#.W7iZanszaM8`

```
Public Class Form1
    Private Sub Timer1_Tick(sender As Object, e
       As EventArgs) Handles Timer1.Tick
        TextBox1.Text = Val(TextBox1.Text) - 1
        If TextBox1.Text = Val(TextBox2.Text)
           Then
            Timer1.Enabled = False
            Timer2.Enabled = False
        End If
    End Sub
    Private Sub Button1_Click(sender As Object, e
       As EventArgs) Handles Button1.Click
        TextBox1.Text = 1000
        TextBox2.Text = 998
        TextBox3.Text = 3
        Timer1.Interval = 1
        Timer2.Interval = 10
        Timer1.Start()
        Timer2.Start()
    End Sub
    Private Sub Timer2_Tick(sender As Object, e
       As EventArgs) Handles Timer2.Tick
        TextBox3.Text = Val(TextBox3.Text) - 1
    End Sub
End Class
```

Daha fazla tekrarlamak ve dolayısıyla beklemek istemiyorsanız, aynı olayı aynı anda daha fazla tekrarlayın. Sayaç sayısını artırırsanız, olasılık artacaktır.[∗]

[∗]Bu basit program bize, her grubun geri sayım süresini rastgele değiştirdiğini gösteriyor. Bazen bir veya birkaçı bazen de diğerleri 1 olur. Tahmin edemezsiniz. Tekrarlar için aynı buton üzerinden istediğiniz frekansı kullanabilirsiniz. Emin olmak için özellikle uzun aralıklı tıklamalar kullanın. Ayrıca otomatik tekrar programı oluşturabilirsiniz. Beklemek istemiyor ve kesin sonuçlar almak istiyorsanız yine aynı kural ile textbox sayısını arttırabilirsiniz. Daha fazla tekrar olan Large Counter.exe adlı programı da aynı adresten indirebilirsiniz.

III. Encoding

Örnekler sayısız olsa da ikinci yöntemi kullanalım.

> *Şimdi, anahtar için İngiliz Alfabesinin kullanıldığını varsayalım. Harflerden 13 tanesi 1 yerine kullanılmak üzere seçilecek ve diğer 13 tanesi 0 için kullanılacak ki; bunlar 0 ve 1 bitleridir.*

Öncelikle örneğin 1 için harfleri seçelim. Bunun için MS Visual Studio Community üzerinden yukarıdaki gibi basit bir program yazdım. Bu programın işlem sonucu öngörülemez ve böyle bir harf ataması için de kullanılabilir. Kendi dilinizi ve kendi yazılım veya donanım mimarinizi kullanarak kendi zamanlayıcınızı yazabilir veya başka bir dil kullanabilirsiniz. Bunlar çok hassas olur ve böylece daha iyi sonuçlar alabilirsiniz. Bu sadece örneğin.

Şimdi her harf için 26 adet zamanlayıcı olduğunu varsayalım. Düğmeye tıklayın veya Büyük Zamanlayıcı üzerinden en az bir tanesi 1 olana kadar işlemi otomatik bir programla tekrarlayın. birden fazlası 1 olursa, sadece birisi 1 olana kadar ve sadece farklı grup için tekrar edeceksiniz. Sonunda birinci kodlama biti için 1 harf seçtiniz. Bundan sonra geri kalan, yani mevcut diğer 16 harf, bit 0'ı kodlamak için kullanılacaktır.

IV. Çevrimdışı Kalibrasyon

> *Harfler üzerinden bit 1 ve bit 0 için anahtar belirlenirken haberleşme için birbirine bağlanması amaçlanan iki bilgisayar aynı anda her ikisine de ilk anahtar kaydedilir ve daha sonra çevrimiçi hale gelirler. Makineyi inşa eden sistem mimarları bile anahtarı bilemez.*

Şimdi, her bir iletişim parçasının belirli bit uzunluklarıyla gerçekleştirildiğini varsayalım. Yani iki bilgisayar, veriler bundan daha kısa olsa bile her zaman 10 KB'lık veri parçaları gönderir. Her 10 KB'lik paketten sonra anahtar değişir. Değiştirici bilgisayar yeni anahtarı gönderir; ancak bu yeni anahtar da bir önceki anahtar üzerinden son kez belirlenir. Bu önceki anahtar zaten rastgeleydi yani sistem mimarları bile bilmiyor. İkinci bilgisayar yeni anahtarı alır ve önceki anahtara göre açar. Bu da bu şekilde sürekli kendini tekrar eder. Yani iki bilgisayarın ne yaptığını kimse bilmiyor. Onları sırdaş yaptık. Saldırılar bile iletişimi ve paketleri bozabilir ama biz iletişim kuramasak bile bizden çalamazlar. Bir dahaki sefere yaklaşık olarak anahtarın ne olacağını kimse bilemeyecek.[†]

V. Uzaktan Kalibrasyon

> *Herhangi bir sinyalin üçüncü bir bilinmeyen bilgisayar tarafından kaydedildiğini düşünüyorsanız, bu tehlikeli olabilir.*

En kötü ihtimalle, bir kullanıcının bilgisayarların ve yazılımın kopyasını yakalamak için belki yeni donanım mimarisini kullanarak herhangi bir eylemi kaydettiğini ve herhangi bir olasılık üzerinden bazı algoritmalarla iletişimin simülasyonunu yaptığını düşünün. Yani onları mantıklı kılmaya çalıştığını varsayın.

Burada da "mutlak" olmasa da aslında çözüm, veri paketlerini küçültmek ve böylece anahtar değişikliğini en sonunda sadece uzaktan kalibrasyon sırasında yüksek frekansta yapmaktır. [‡]

Böylece yakalanma olasılığı düşecektir.

[†]Yalnızca kalibrasyonu kaydetmek de çözüm değildir hack için. Herhangi bir eylemi her zaman kaydetmelisiniz. Hırsız veya kötü niyetli bir mühendisseniz, baştan kayıt sırasında iletişimin ömrü boyunca yalnızca bir 10 KB'lık paket kaybederseniz, hiçbir şey yapamazsınız.

[‡]Mutlak değil demek, teoride bir yorumdur. Uzaktan da olsa kalibrasyon ve sistem dinlense bile olasılığı çok düşüktür hack işleminin.

VI. Sonuç

Görüldüğü gibi her bilgi ve aranan bilgi bize göre bir noktadan sonra aynı hale gelmektedir. 1 veya 0 gibi kodlama için yalnızca bir bitiniz varsa, herhangi bir harfi alabilir. Yani 1 veya 0 için 26 olasılık vardır. 10, 11, 01 veya 00 gibi bir bit grubunuz varsa, her biri aynı harfleri alabilir. "Rastgele seçilen anahtarı" bilmiyorsanız hangisinin asıl amaç olduğuna karar veremezsiniz. Koşul, herhangi bir uzunluk bit grubu için aynıdır. 1 ve 0 için her 16 harf arasında ikinci bir seçim yapıldığını unutmayınız. Yani bir bit grubundaki her 1 için 16 harften 1 tanesi rastgele seçilecektir. Yani bir hacker'a göre 1 veya 0 herhangi bir harf alabilir. Çalınan bilgiler her anlama gelebilir.

> *Anahtar da rastgele belirlenir. Oluşturucu sistem mimarı insanlar da anahtarın ne olacağını bilemezler. Yaklaşık bir tahmin de mümkün olmayacaktır. Aniden en kötü ve öngörülemeyen olasılık olabilir. Yani anahtar için mühendisleri kaçırmak ve tehdit etmek fayda sağlamaz.*

Bu yapının en iyi şekilde çalışması için aslında yeni bir donanım desteği gerekiyor. Özellikle bazı özel iletişim araçları için, yeni bir donanım mimarisi oluşturmalısınız ve ardından donanım, bilinmeyen yeni donanım karakterleri veya frekansları üzerinden seçim yapacaktır. Buna rağmen, bazı basit programlar tarafından yapılan rahatsız edici saldırıların çoğunu engelleyebilir. Örneğin, basit bir Windows öykünücüsü bunu engelleyebilir. Tüm pencereler önce basit bir kodlama programı üzerinden çalışacak. Bilgisayarlar bile bir key-logger yazılımına veya e-postaya anlamsız karakterlerle cevap verecek. Yani aslında bizden çalabilirler ama o bilginin ne anlama geldiğini bilemezler. Herhangi bir bilgi olabilir.

18.06.2023