NİCEM HESAPLAMA (QUANTUM COMPUTATION) VE BİLGİ GÜVENLİĞİNİN YENİ ROTALARI

Alp ÖZTARHAN[1] **Aydın KUBİLAY**[2] **Devrim ÜNAL**[3]

[1-3]Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
P.K. 74, 41730, Gebze, Kocaeli

[1]ileti: alp@uekae.tubitak.gov.tr
[2]ileti: akubilay@uekae.tubitak.gov.tr
[3]ileti: devrimu@uekae.tubitak.gov.tr

Anahtar sözcükler: Nicem Hesaplama, Quantum Computation, Karmaşıklık Teorisi, Bilgi Güvenliği

• ABSTRACT

This paper is about an esoteric topic not considered much in data security, but should. The topic, Quantum Computation is introduced and its consequences are discussed. After a brief introduction and history, the limits on what can be done in this field follows. The discussions of the paper is limited to the field of cryptography, and a transformation is proposed in the field. A first suggestion is a shift towards information theory, which is followed by a conclusion discussing some consequences also.

1. ÖZET

Bu bildiride, Nicem Hesaplama tanıtılacak ve bilgi güvenliği alanına etkileri tartışılacaktır.

Nicem hesaplamanın bir tanıtımı ve tarihinden sonra, bu yeni alanla başarılabileceklerin sınırları üzerinde durulacaktır. Bildirinin savı, bilgi güvenliği alanında tüm klasik kavramların elden geçirilip bazı dönüşümlerin yaşanması gerektiğidir. Konunun genişliğini dikkate alarak, bildirinin tartışmaları ve çözüm önerileri bilgi gizleme (kriptoloji) alanı ile sınırlandırılmış; bu alanda yaşanması gereken dönüşümlere dair bazı öneriler de yazıya eklenmiştir. Bilindiği gibi şu ana dek ağırlıklı olarak kullanılan bilgi gizleme yöntemleri, hesaplama güçlüğüne dayanır. Ele alınan öncelikli öneri, bu geleneksel tarzın terk edilmesidir. Çözüm olarak bilgi kuramına (information theory) dayalı yöntemler önerilmiş, son bölümde de bu yöntemler sonuçlarıyla tartışılmıştır.

2. NİCEM HESAPLAMA NEDİR?

Nicem fiziği (Quantum Physics), yirminci yüzyılın bilimsel alanda en önemli buluşlarından biridir. Doğanın kavranışında radikal dönüşümler getiren bu bakışa göre, bizim gündelik yaşamda alıştığımız ve doğanın davranış biçimi olarak kavrayıp pek sorgulamadığımız genellemeler, atomlar ve atomaltı parçacıklara doğru küçük ölçeklerde çalışmaya başladığımız oranda geçerliliklerini yitirmektedir.

Örneğin kedimiz ya evimizde ya da dışarıdayken, nicem dünyasında bir elektron hem A yörüngesinde hem de B yörüngesinde yer alabilmektedir. Bu özelliğe "üst üste binme özelliği"[1] diyebiliriz.

Yine alışılmadık bir durum, fiziksel sistemleri parçalarının toplamları olarak ele alma alışkanlığıdır. Bu alışkanlığa göre, fiziksel bir sistemi kavramak için bir yöntem, tek tek tüm parçaların içinde bulundukları durumu kavramaktır.

Oysa nicem fiziğinde sistem, parçaların toplamından çok daha fazla bir şeydir. Sistemde parçaların yanı sıra tüm parça ikililerinin, üçlülerinin ve her türlü kombinasyonun diğer kombinasyonların dışında, kendilerine özgü durumları mevcuttur. Yani iki parçacığın etkileşimine dair bilgiyi, o parçacıklara dair her şeyi bilsek bile bilemeyiz. Ayrıca o ikiliye dair etkileşimi de incelememiz gerekir. Daha da çarpıcısı, üç parçacığın etkileşimini bilmek için tek tek her parçanın, ve her bir ikilinin etkileşimine dair herşeyi bilmenin yetmemesidir. Bir de o üçlünün etkileşimine dair özel bir bilgi daha vardır ve ona da bakılması gerekir.

Nicem fiziğinin İlşkilerin sayısının ilişkiye giren parçaların sayısından çok daha hızla artması özelliği

[1] Bu bir ***dağılma*** özelliği değildir. Elektronun biraz orada biraz burada olduğunu düşünmek de yanlış olacaktır. Doğrusu, elektronun ***iki yerde birden*** olduğudur. Buna dair verilebilecek iyi bir örnek, olası değişik rotalardan geçerek bir noktaya gelen elektronun aldığı halin, tüm olası yollar üzerinde olan çeşitli durumları içinde barındırmasıdır. Yani elektron tek bir yoldan gidilebilecek bir zamanda hepsinden birden geçmiş ve her yol üzerinde ne varsa hepsini birden görmüştür.

bu tür sistemlerin bilgisayar benzeşimini yapmayı çok güçleştirmektedir. Öyle ki, bugün makul sürelerde çok küçük boyun biraz üzerinde bir sistemin dahi benzeşimi yapılamamaktadır.

Oysa sistemin kendisi bu hesaplamayı çok kısa sürede gerçekleştirebilmektedir. Bunu sağlayan, üst üste binme özelliğidir. Bu davranışta bulunan madde, olası durumların hepsine bakıp beğendiğinde karar kılma şansına sahiptir. Nicem hesaplamanın kullanmaya çalıştığı özellik de tamı tamına budur. Böylelikle eleman sayısının üstü karmaşıklıkta problemlere girişmek olanaklı gözükmektedir.

3. NİCEM HESAPLAMANIN TARİH ÖNCESİ

Nicem hesaplamanın bir uğraş alanı olarak ortaya çıkışında iki koldan gelişen olayların etkisi vardır. Birinci kolda, elektronik alanındaki (üstel olduğu öne sürülen)[2] yüksek hızda bir küçülme vardır. Aynı işi yapan devreler her geçen yıl daha da küçülmekte ve devre elemanları küçüldükçe nicem etkilerinin önemi artmaktadır.

İkinci kolda ise hesaplamalı fizikçilerin nicem olaylarının benzeşiminde (simülasyon) karşılaştıkları güçlüklerdir. Bu güçlükler şunu göstermektedir: Alışıldık bilgisayarlarla hesaplanamayan bu problemler, fiziksel süreçler tarafından hızla yerine getirilebilmektedir. Öyleyse bazı fiziksel göstergeler bazı problemler için alışıldık bilgisayarlardan daha hızlı bir çözümü oluşturabilmektedir.

4. NİCEM HESAPLAMANIN SINIRLARI

Nicem hesaplama başlangıçta çoğu araştırmacı için yalnızca ilginç ve pek pratik sonuçları olmayan bir araştırma dalı idi. Bu durumu değiştiren en önemli etkenlerden biri, 1994 yılında Peter W. Shor'un yayınladığı [7] nicem hesaplama yöntemleri oldu.

Shor, söz konusu makalesinde, bir nicem bilgisayar üzerinde, makul sürede çarpanlarına ayırma ve ayrık logaritma alma yöntemlerini gösterdi.

Çarpanlarına ayırma ve ayrık logaritmanın klasik bilgisayarlarda makul sürede yapılamayacağına dair güçlü birer inanış olduğu için, bu sonuç araştırmacıları nicem bilgisayarların sınırlarını aramaya sevk etti.

Karmaşıklık Kuramı (Complexity Theory) bilgisayarlarda makul sürede yapılabileceklerin sınırlarını belirlemede yol gösteren önemli bir kuram olarak nicem bilgisayarlardan önemli ölçüde etkilendi. [8,9]

Problemlerin hangi sürede çözülebileceğine dair elimizdeki bilgiler sınırlıdır. Gayet gelişkin tahminlerde bulunabilmek için yeterince veri bulunmakla birlikte, yine de bunlar birer tahmindir. Bu alanın şaşırtmacalardan uzak olduğunu söylemek de pek mümkün değildir.

Kısaca söylenebilecekler şunlardır:

- Klasik bilgisayarlarda makul sürede yapılabileceklerin sınırı pek çizilememiştir.
- Yine de, pek çok problemin klasik bilgisayarlarda makul sürede yapılamayacağına dair güçlü bir kanı oluşmuştur.
- Bu problemlerin bazılarının nicem bilgisayarlarda makul sürede nasıl çözülebileceği gösterilmiştir. Bu, nicem bilgisayarların öneminin bir pratik göstergesidir.
- Klasik bilgisayarda girdi büyüklüğü ile orantılı olduğu kanıtlanabilecek bir problemin, nicem bilgisayarlarda karekökle çözülebileceği gösterilmiştir. Bunun önemi, nicem bilgisayarların klasik bilgisayarlardan en azından bir alanda üstün olduğunun kanıtını oluşturmasıdır.
- Nicem bilgisayarların yeteneklerine dair yeni buluşlar yapılmaya devam etmektedir. Bu da elimizdeki problemlerin nicem bilgisayar tarafından kırılmalarının güçlü bir potansiyel olduğu anlamını taşır.

5. HESAPLAMA GÜÇLÜĞÜNÜN ÖNEMİ AZALMIŞTIR

Hesaplama güçlüğüne dayanan gizleme yöntemlerinden kaçınmanın günümüzde artık haklı nedenleri vardır. Çünkü:

a) Hesap güçlüğünün sınırları her geçen gün yükseliyor. Bu yükseliş üstel olduğu için efektif olarak bir anahtarın kırılması anahtarın uzunluğu mertebesinde (doğrusal) olacaktır.

b) Nicem bilgisayarlar bu yöntemlerin önemli bir kısmını kuramsal olarak kırmıştır. Bu ifadeyle kastedilen, istenilen niteliklerdeki bir nicem bilgisayarın gerçekleştirilmesi ile bu yöntemlerin (kolaylıkla kırılacağı için) artık kullanılamayacağıdır. Üstelik gün geçtikçe bu şekilde kırılan problem sayısı da artmaktadır. Henüz nicem bilgisayarların çözebileceği problemlerin sınırlarını pek bilmiyoruz. (Aynı sorun normal bilgisayarlarda da olmakla birlikte, bazı problemlerin çözülemeyeceğine dair güçlü kanılar mevcuttur. Bu tür problemlere bir örnek, çarpanlarına ayırma problemidir.) Daha da önemlisi, henüz elimizde nicem bilgisayarlarla çözülemeyeceğine dair güçlü bir inanç oluşturan bir problem de yoktur.

c) Nicem bilgisayarlar yokken dahi elimizdeki güvencenin en fazlası, bazı problemlerin makul sürede çözülemeyeceğine dair güçlü inançtır. Hesaplama güçlüğü için kullandığımız problemlerin hiçbirinin hiçbir zaman çözülemeyeceği gösterilememiştir. Şu anki koşullarda çözülmeleri şaşırtıcı olacaktır ve çözülmeyeceklerini sanmak için yeterli

[2] Moore yasası, söz konusu hızın üstel olduğunu öne sürer ve 6. bölümde ele alınacaktır.

gerekçelerimiz vardır. Fakat teknoloji seviyesine bağlı belirsizlik ve sonucu bilememe sıkıntısı çok rahatsız edicidir.

d) Nicem bilgisayarlar, fiziksel süreçlerin bildiğimiz hesaplama modellerine uymak zorunda olmadığının önemli bir örneğidir[3]. Bırakın hesaplama güçlüğü ve hesap için uzun süre gereksinimi sorunlarını halletmesini, fiziksel süreçlerin Turing makinesiyle hesaplanamayacağı kanıtlanmış problemleri çözemeyeceğinden dahi emin olamayız. Nitekim ünlü fizikçi Roger Penrose, bu tür fiziksel süreçlerin insan beyninde rol aldığını öne sürmektedir.[2]

Bu nedenle zaman içinde güvenlik gereksinimlerinde bilgi kuramsal (information theoretic) yaklaşımların kullanımı önem kazanacaktır.

6. HESAPLAMA GÜÇLÜĞÜ DOĞRUSALI AŞAMIYOR

Moore Yasası, Intel'in kurucularından Gordon Moore'un 1965'te yaptığı bir gözlem ve öngörüsüne dayanmaktadır. Buna göre, entegre devrelerdeki transistor sayısı, her geçen yılda katlanmaktadır. [4,5]

Moore, daha sonra 1975 yılında öngörüsünü değiştirmiş ve katlanma süresini 2 yıl olarak önermişti. Intel ve popüler medyada bu süre 18 ay olarak verilmektedir.

Konunun bilimsel incelemeleri, Moore yasasının muğlaklığı nedeniyle pek güçtür. Yasa muğlaktır, çünkü Moore (ve Intel) önceleri üretim teknolojilerindeki gelişmelere işaret ederken, sonraları tasarım teknolojisine kaymıştır. Şimdilerde ise en yüksek teknolojili devrelerin eleman sayılarından, birim hesaplama gücünün fiyatına dek değişik ölçütlerden söz edilmeye başlanmıştır.

Öngörüyü sabitlemeye çalıştığımızda ise, pek başarılı olmadığı söylenebilir. Örneğin optimum fiyatta üretilen devrelerin küçülmesine dair yapılan özgün öngörü önceleri bir yıldan iki yıla çıkmıştır. Bugün, söz konusu katlamanın ölçümleri 54 aya (4.5 yıl) varmaktadır.

Moore yasası, kendi varlığı ile bir basınç oluşturmakta, bu basınç üzerinden örneğin bellek büyümesi, hız artışı, devre küçülmesi, birim hesaplamanın fiyatının düşüşü vb. ölçütlerin hepsi logaritmik olarak değerlendirilmektedir.

Çok sağlam olmasa da, yine de, bu değerlendirmenin gerçek bir yanı mevcuttur. Son otuz yıldır hesaplamaya dair çeşitli bileşenlerin katlanarak ucuzladığı söylenebilir. Hız artışı tam üstel olmasa da polinomsal da değildir. Kaba bir ölçütle üstel hızın korunduğunu düşünebiliriz. Bu hız otuz yıldır sürmektedir ve önümüzdeki yıllarda azalacağını öngörmek için eldeki nedenler, çoğalacağına dair nedenlerden daha ikna edici değildir.

Eğer Moore yasasını geçerli kabul edersek, bir şifrenin kırılması için gerekli karmaşıklık doğrusalın altında çıkacaktır. Bu çarpıcı sonuç, tüm anahtarların denenmesinin doğrusal karmaşıklıkta olmasından kaynaklanmaktadır:

Anahtar uzunluğu x olan bir gizleme yöntemimiz olduğunu varsayalım. Yine varsayalım ki bir birim zamanda (T) bir gizleme (veya açma) yapabilmekteyiz. Moore yasasına göre, (diyelim ki "k" birimlik bir katlanma süresi aldık) "kx" birim zaman içinde, bir birim zamanda tüm anahtarları denemek olası olacaktır. Anahtara bir bit daha eklemek, çözülme süresini katlamayacak, yalnızca sabit bir "kx" süresi kadar uzatacaktır.

Bu elbette çok pratik bir yöntem değildir. Ancak hesaplama güçlüğüne yaslanmanın sorunlarına dair ek bir göstergedir.

7. BİLGİ KURAMI BİR ÇÖZÜM SUNABİLİR Mİ?

Shannon, 1949 tarihli ünlü makalesinde [10] iki önemli kavram tanımlamıştır. Bunlardan birincisi kusursuz gizlem (perfect cipher), ikincisi ise ideal gizlemdir (ideal cipher).

Kusursuz gizlem, kapatılmış metnin ele geçirilmesinin, ele geçiren yetkisiz kişiye ek hiçbir bilgi vermemesi anlamına gelir. Shannon, bu durumun ancak anahtar uzayının mesaj uzayından büyük (veya eşit) olduğu durumlarda olanaklı olduğunu göstermiştir.

İdeal şifrelerin tanımı ise, ne uzunlukta kapalı mesaj alınırsa alınsın, anahtar uzayındaki olası anahtarların yeterince daralmamasına dayanmaktadır. Yeni yetkisiz kişiler dinledikleri mesajları olası bazı anahtarlarla açtıklarında olası birden fazla açık mesaj görecekler, asıl mesajın ne olduğundan hiçbir zaman emin olamayacaklardır.[4]

İdeal gizlemler, varlıkları bilinmekle birlikte üzerlerinde fazla durulmamış sistemlerdir. Bilgi kuramı, bilgi gizleme alanında zor olan yoldur. Hesaplama güçlükleri ise şimdiye dek kolaylıklarından ötürü popülerliklerini sürdürmüştür.

Geleceğin bilgi gizleme yöntemlerinde öne çıkması beklenen bilgi kuramsal yöntemler, mesaj uzayının ve

[3] Bu konuda bir başka örnek olarak sabun köpüklerinin hesaplama yetenekleri ele alınabilir. Bir yüzeyin köşeleri bir tel aracılığıyla oluşturulup sabunlu suya daldırıldığı zaman oluşan sabun köpükleri, söz konusu köşelerden geçen minimum alanlı yüzeyi oluşturmaktadır. Oysa bu yüzeyin makul sürede gerçekleştirilebilen bir bilgisayar hesap yöntemi bilinmemektedir. [3]

[4] Bu tanımlar, hesaplama güçlüğünü konu dışında bırakıyor. Tanımlarda bu tür mesajların hesaplanabilirliği değil, ***varlığı*** üzerinde durulmaktadır. Bu da sonsuz hesap gücü olan bir yetkisiz kişi için dahi bir kısıt oluştuğu anlamına gelir. Bilgisayar ne kadar güçlü olursa olsun, yetkisiz kişi elindeki olası mesajlardan hangisinin gerçek mesaj olduğunu bilemeyecektir.

mesajların yapısına dair bilgilerin yarıştırıldığı bir alana dönüşecektir. İdeal gizlemlere benzeyen yapılar sayesinde anahtarların ömrü uzatılacaktır.

Ancak gizleyenle yetkisiz olarak çözmeye çalışan arasında çözen lehine bir asimetri vardır. Çoğu durumda çözenin gizleyene oranla çok daha fazla zamanı vardır. Bu etken de anahtarın ömrünü kısaltıcı bir etki yapmaktadır. İdeal sistemlerde anahtar ömrü sınırsız olmakla birlikte, bu etkenler de göz önünde bulundurulursa toplamda anahtar ömrü sınırlıdır.

Bu sorunun çözümü için görülen tek yöntem; anahtar akışının sürekliliğidir. Sınırlı ömrü olan anahtarlar, sık sık değiştirilmeli, askeri uygulamalarda standart olan anahtar değiştirme yöntemleri ve lojistikleri, aynı yöntemlerle olmasa da sivil yaşamda benzerleri oluşturulmalıdır. Bu tarz bir çalışmayı olanaklı yapan, bilgi kuramsal çalışmalarla anahtar ömrünü oldukça anlamlı uzunluklara çekmenin olanaklı görünmesidir.

• KAYNAKLAR

[1] Gruska, Jozef, Quantum Computing, Mc Graw Hill, 1999

[2] Penrose, Roger; "Shadows of the Mind", Oxford University Press, 1996

[3] Chiu, Daniel T.; Pezzoli, Elena; Wu, Hongkai; Stroock, Abraham D., Whitesides, G. M., "Using three-dimensional microfluidic networks for solving computationally hard problems", ABD Ulusal Bilimler Akademisi Bildirisi, Cilt 98, No: 6, 13 Mart 2001 (http://www.pnas.org/cgi/content/full/98/6/296)

[4] Wikipedia, Moore Yasası hakkındaki makale, (http://en.wikipedia.org/wiki/Moore's_law)

[5] Intel'in Moore Yasası web sayfası (http://www.intel.com/research/silicon/mooreslaw.htm)

[6] Tuomi, Ikka, The Lives and Death of Moore's Law, First Monday, Cilt 7, Sayı 11, (http://firstmonday.org/issues/issue7_11/tuomi/index.html)

[7] Shor, Peter W.; "Polynomail Time Algorithms for Prime Factorization and Discrete Logarithms On a Quantum Computer", Proceedings on the 35th Annual Symposium on the Foundations of Computer Science (http://www.imsc.ernet.in/tcsweb/quantum/shor-focs.ps)

[8] Goldreich, Oded; Introduction to Complexity Theory, (http://www.wisdom.weizmann.ac.il/~oded/cc.html)

[9] Aaronson, Scott; Complexity Zoo (http://www.complexityzoo.com)

[10] Shannon, Claude E.; "Communication Theory of Secrecy Systems", Bell Systems Technical Journal, Cilt 28-4, Sayfa 656-715, 1949 (http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf)