



New York Üniversitesi Tandon Mühendislik Okulu'ndaki araştırmacılar, mümkün olan en yüksek düzeyde yapısal rassallığa sahip, düşük maliyetli bir nanomateryalden üretilen yeni bir sınıfa karşı siber güvenlik önceliği tanıttıklarından güncel nesil elektronik donanım güvenliği hazırlanabilir. Rastgele olma, bilgisayar donanımını ve verilerini fiziksel olarak şifreleyen ve böylece programlamadan ziyade güvenlik ilkelleri oluşturmak için çok talep görebilir.

ACS Nano dergisinde yayınlanan bir makalede, Elektrik ve Bilgisayar Mühendisliği Yardımcı Profesörü Davood Shahrjerdi ve NYU Tandon ekibi, atomik olarak ince molibden disülfid (MoS_2) 'de tam uzamsal rassallığın ilk kanıtıdır. Araştırmacılar, nanomateryalleri, her biri insan saçından yaklaşık bir milyon kat daha ince katmanlar halinde büyüttüler. Shahrjerdi, her tabakanın kalınlığını değiştirerek, malzemenin özelliklerini etkileyen enerji bandı yapısının boyutunu ve türünü ayarladıklarını açıkladı.

“Tek katmanlı kalınlıkta bu malzeme, ışık yayan yarı iletkenlerin optik özelliklerine sahip ancak çok katmanlı olarak özellikleri değişiyor ve malzeme artık ışık yaymıyor. Bu özellik sadece bu malzemeye özgüdür” dedi. Malzeme büyüme sürecini ayarlayarak, ortaya çıkan ince film, alternatif olarak ışık yayan ve ya ışık yaymadan rasgele meydana gelen bölgelerle lekelenir. Işığa maruz kaldığında, bu model en düşük maliyetle donanım bileşenlerini güvence altına alabilen benzersiz bir kimlik doğrulama anahtarı haline dönüşür.

Shahrjerdi ekibi, MoS₂'nin rastgele ışık örüntüleri olarak tanımladığı şey için potansiyel başvuruları düşünürken, bir şifreleme ikelliği olarak son derece değerli olacağını düşündüğünü söyledi.

Bu, nanomateryal kullanılarak oluşturulan fiziksel olarak ilk klonlanamayan güvenlik önceliğini temsil eder. Tipik olarak entegre devrelere yerleştirilen fiziksel olarak klonlanamayan güvenlik önceliği, donanım veya dijital bilgileri korur veya kimliğini doğrular. Şifreleme anahtarı veya kimlik doğrulama aracı olarak işlev görebilecek benzersiz bir yanıt üretmek için bir uyarıcı (bu durumda ışığın) ile etkileşime girerler.

Araştırma ekibi, benzeri nanomateryal temelli güvenlik primitiflerinin ucuz ölçekte üretilebileceğini ve bir mektubun posta pulu gibi bir çip ve ya başka bir donanım bileşenine uygulanabileceği bir geleceği düşünüyor. Shahrjerdi, "Herhangi bir metal temasa gerek duyulmadığı gibi üretim de çip imalat sürecinden bağımsız olarak gerçekleşebilir" dedi. "En az yatırımla maksimum güvenlik" dedi.

ACS Nano dergisinde "Katmanlı MoS₂'nin kimyasal buhar birikimi ile fiziksel olarak klonlanmamış kriptografik primitifler" gazetesinde yer almaktadır.

Kaynak : phys.org

Yorumlar