GİZLİ HABERLEŞME KUANTUM KRİPTOGRAFİ ÂLETİ

Temmuz 1992'de başlatılan bir çalışmayla matematiğin ulaşamadığı düzeyde şifreleme başarısını kuantum mekaniği, ışık kuantumları olan fotonlarla sağlıyor. Heisenberg belirsizlik kuralına dayanan bu şifreleme sisteminde her türlü düşmanın ya da karşıtın çözemeyeceği bir güvenilir kodlama yapılmaktadır.

2500 yıldır örnekleri bulunan gizli haberleşme ve şifreleme tarihin her döneminde çok önemli işlevler yerine getirmiş ve çok önemli olayların gelişmesini etkilemiştir. Örneğin Amerika Birleşik Devletleri'ni Birinci Dünya Savaşı'na girmeye zorlayan da böyle gizli şifrelenmiş bir mesajın açığa çıkması olmuştur.

İşte bu sıralarda Amerika Birleşik Devletleri PTT sinde görevli Gilbert S.Vernam ile Amerikan Ordusunda görevli Binbaşı Joseph O.Mauborgne düşmanlarınca çözümlenemeyecek bir şifreleme sistemi geliştirdiler. Vernam şifresi denen bu sistemde, şifre ile anahtarı aynı uzunlukta ve blok halinde bulunuyor ve ancak bir kez kullanılıyordu. Şifre anahtarı blok halinde şifreyi taşıyana verilmekte ve şifre bloğunun yaprakları bir kez kullanıldıktan sonra yok edilmekteydi. O sıralarda kullanışlı sayılan ancak çok yer tuttuğu için çok uzun bulunan bu şifreleme yerine diplomatlar ve gizli haberleşme yapan kişiler daha kısa ve kolay yöntemler kullandılar. Almanların ve Japonların İkinci Dünya Savaşı'nda çok ağır bir yenilgi almalarında şifreleme sistemlerinin karşıt devletlerce kolayca çözülmesi çok etkili oldu. Bu arada gizli şifreleme bilgisayarı geliştirdi. Bilgisayar ise giderek daha hızlı ve güvenilir şifrelemede kullanılır oldu. Kriptoloji adında şifreleme bilgileri özellikle 70'li yıllarda Kaliforniya'nın Stanford Üniversitesi'nden Whitfield Diffie, Martin E.Hellman ve Ralph C. Merkle kamuya açık kripto sistemleri ilkelerini açıkladıktan sonra (public - key cryptography, PKC) gelişmeler hızlandı. 1977 yılında Massachusetts Teknoloji Enstitüsü'nden (MIT) Ronald L.Rivest, Adi Shamir ve Leonard M.Adleman bu sistemin uygulama alanlarını genişlettiler. Ancak daha kesin ve kullanışlı sistem arayışları da sürmekteydi. 1970'lerde Columbia Üniversitesi'nden (New York) Stephan J.Wiesner klasik fizikle mümkün olmayan, ancak kuantum etkisiyle işleyen "çekilmiş simgelem: conjugate coding" adını verdiği bir yeni sistem geliştirdi. Ancak Wiesner'in çalışması 1983 yılına kadar yeterli ilgiyi görmedi. Bu arada Bennett ve Brassard adlı araştırmacılar kamuya açık "simgeleme ile Wiesner'in yeni kuantum tekniğini bağdaştırmaya çalıştılar. 1991 yılında çok güvenilir şifreleme sağlayan kuantum mekaniğine dayanan cihaz yapıldı. Burada verici kısmı polarize edilmiş ışığı ölçümleyerek gizli bilgileri güvenilir biçimde iletmede kullanıyor. Işık yoğunluğu öyle seçiliyor ki, her onuncu ışık darbesi bir foton tarafından aktarılabilmektedir. Böylesine güvenilir şifreleme olanağı bulunca bu sistemi kullanan diplomatlar, bankacılar, mühendisler, ordu ve emniyet görevlileri, şifrelenmiş mesajlarını açıkça vermekte hatta gazete ilanları şeklinde vermekte ancak şifreyi çözecek anahtar çok gizli iletilmektedir. Yeni yöntem geliştirilirken, hâlâ Moskova ve Washington arasında Vernam şifre sistemi kullanılıyor. Ticarî şifrelemelerde ise kısa adı DES olan Data Encyripton Standard kullanılıyor. Buysa gizli 56 bit anahtarı olan ve çok fazla haberleşme mesajı için belirli bir süre geçerli olan bir sistem. Ancak bu tür sistemlerin alıcısına ulaşmadan ele geçirilerek çözümlenmesi tehlikesi bulunuyor.

GİZLİ ŞİFRELEMEDE YENİ YÖNTEM: KUANTUM MEKANİĞİ

Klasik fizikte olduğundan farklı bir şekilde kuantum kuramına göre verici tarafından bir ışık polarizasyonu filtresi kullanmak suretiyle fotonlara bilgiyi yüklemek ve alıcı tarafından bu bilgiyi çözerek mesajı deşifre etmek mümkün oluyor. Yatay polarize olmuş fotonlar kalsit kristalinden geçirilerek değerlendiriliyor. Tüm bu çabalar yalnızca gizli iletişimi en güvenilir biçimde gerçekleştirebilmek için. İnsanlık bir gün her türlü sorunun kaynağını oluşturan savaşları, yapay rekabet ortamlarını ortadan kaldırırsa, artık gizli iletişime de gerek kalmayacak.

Spektrum der Wissenschaft Aralık 1992'den
çev.: Doç.Dr. A.Tamer ÜRÜM

mesinde, 5-6 yıl gibi uzun bir zaman alan geriye melezleme metotları kullanılmaktadır. Bitki doku kültürleri teknikleri bu alanda da ıslahçıya yardımcı olabilmektedir. Erkek kısırlık genelde hücre çekirdeği (nüklear erkek kısırlık) ve sitoplazmadaki (sitoplazmik erkek kısırlık) mitokondrilerde bulunan genler arasındaki ilişkiler sonucunda ortaya çıkmaktadır. Protoplast füzyon tekniği kullanılarak bir bitkiden diğer bir bitkiye erkek kısırlık aktarılabilmektedir. Örneğin, erkek kısırlık karakteri *Nicotiana tabacum*'dan *Nicotiana sylvestris*'e bu yolla aktarılmıştır. *N.tabacum* protoplastları önce x-ışınları ile radyasyona tâbi tutulmuş, dolayısıyla nükleer DNA parçalanarak işlemez hale getirilmiştir. Daha sonra *N.sylvestris* protoplastları ile füzyon edilerek fonksiyon gösteren mitokondrial DNA, dolayısıyla sitoplazmik erkek kısırlık aktarılmıştır. Elde edilen hibrit protoplastlar yeni bitkilere dönüştürüldüğünde, bitkilerin çiçeklerinde pollen tozları gelişememiştir. Bu tip çalışmalar, dünyadaki birçok labaratuvarlarda rahatlıkla diğer bitkilerde de, örneğin mısır bitkisinde gerçekleştirilmekte ve özellikle büyük tohum firmaları tarafından çok kullanılmaktadır. Son iki yıl içerisinde ise erkek kısırlığa sebep olan gen izole edilerek diğer bitkilere de aktarılmıştır. Bu da geleneksel yolla yapılan geriye melezlemeyi ortadan kaldırdığı gibi, ıslah çalışmalarına da büyük bir katkı sağlamıştır.

Görüldüğü gibi, bitki doku kültürleri teknikleri, bitkilerin ıslahında ve tarımsal özelliklerinin iyileştirilmesinde büyük bir rol oynadığı gibi, ıslahı gerçekleştirilmiş ve istenilen düzeye eriştirilmiş bitki materyallerinin de hızla üretilerek, elit bitki bekleyen üretici çiftçiye bir an önce ulaşmasında yardımcı olmaktadır. Bunlardan başka, bitkilerin genetik transformasyonu esnasında çok kullanılan metotlardan birini oluşturmaktadır.