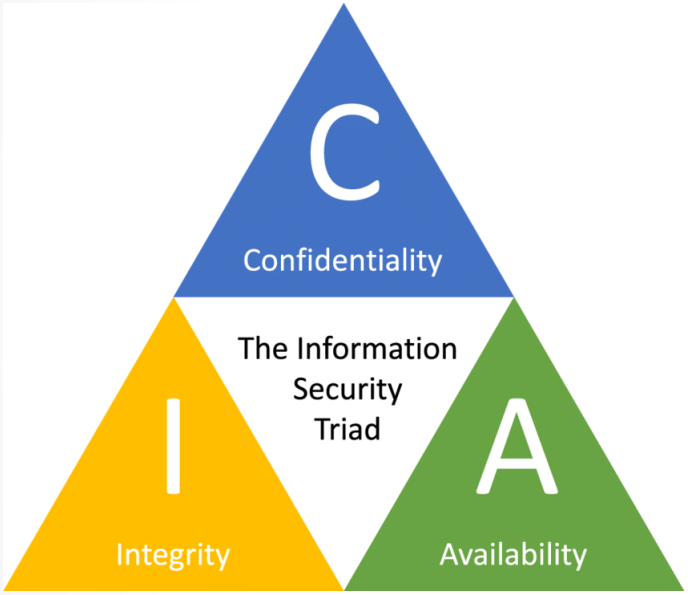
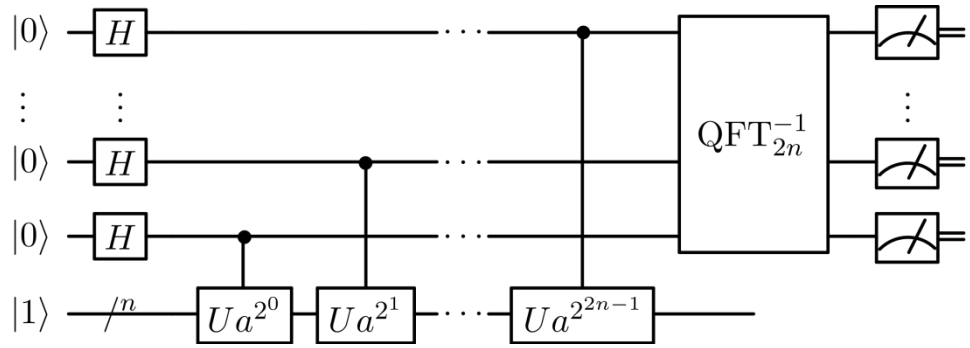
DNA Origami Cryptography For Secure Communication

- Biyomoleküler kriptografi verileri şifrelemek için biyomoloküler etkileşimlerden yararlanır. Bu da bigi güvenliği için farklı ve benzersiz bir yaklaşımı temsil eder. Bununla birlikte bilginin gizliliği, bütünlüğü ve erişlebilirlik için biyomoleküler reaksiyonlara dayanan protokoller oluşturmak hala yeterince güvenilir değil.

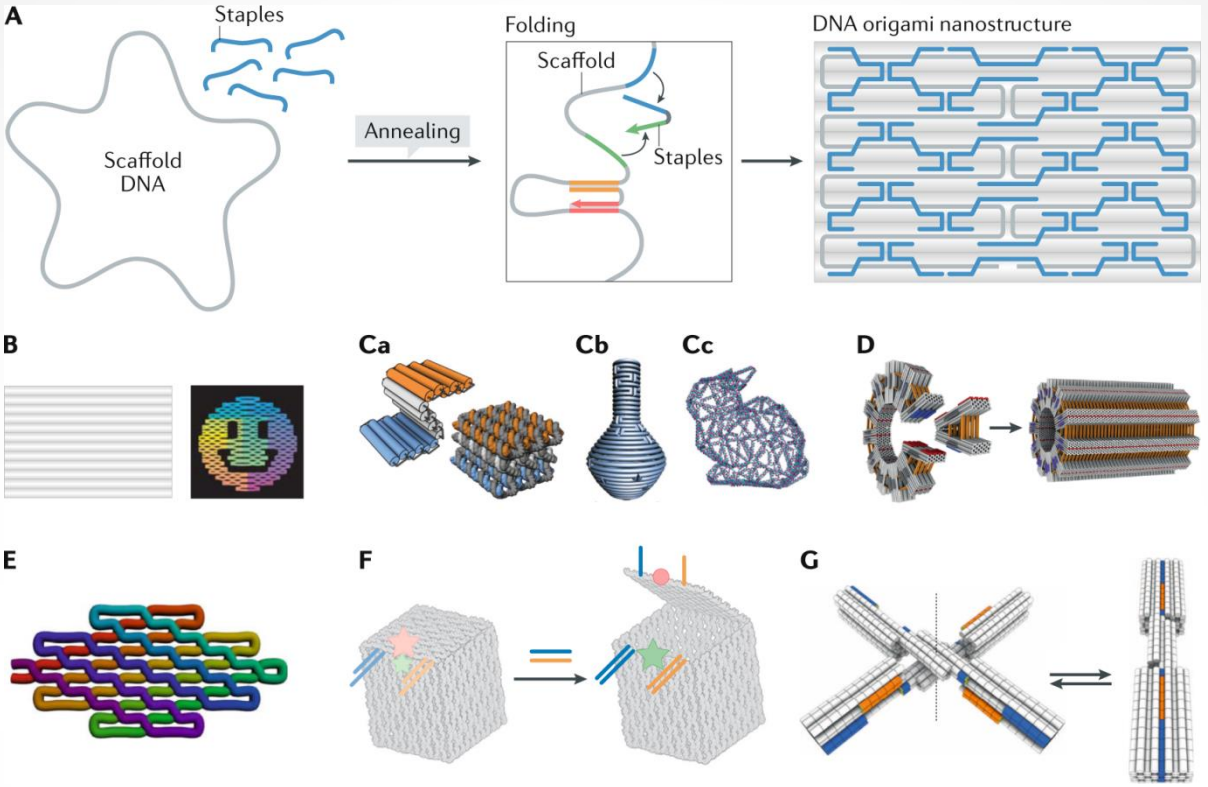


- Bilgi güvenliği (CIA üçlüsü)- gizlilik(confidentially), bütünlük(integrity) ve kullanılabilirlik(availability- modern toplumda çok önemli bir rol oynar.
- Bu talebi karşılamak için, zorlu hesaplama problemlerine dayanan karmaşık kriptografi şemaları oluşturulmuştur. Bununla birlikte mevcut kriptografi protokolleri ciddi zorluklarla karşı karşıyadır.

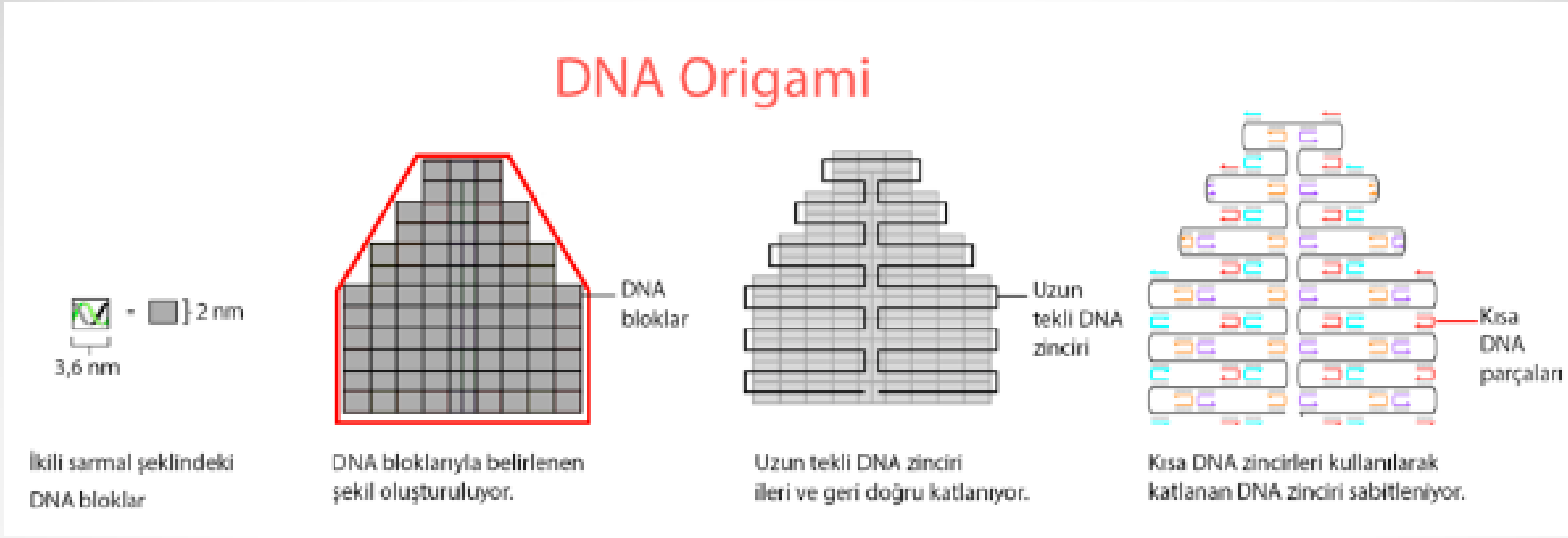
- Bilgisayarların devam eden gelişimi ile şu anda kullanılan kriptografi protokollerinin kaba kuvvet(brute-force) saldırılarıyla kabul edilebilir bir süre içinde kırılmasına olanak sağlıyor.
- Bir diğer yandan kuantum bilgisayarların ortaya çıkışı, Shor'un algoritması aracılığıyla da anahtarların kolayca kırılmasına izin verecektir.



- Özellikle, kuantum kriptografi yöntemleri, mesaj gizliliğini sağlamak için büyük umut vaat ediyor olsa da bilgi güvenliği temel unsurlarının kuantum iletişimi yoluyla kapsamlı bir şekilde elde edilip edilemeyeceği hala belirsiz bir konu.
- Biyomoleküler etkileşimleri kullanan biyomoleküler kriptografi, daha önce bir alternatif olarak önerilmiş.

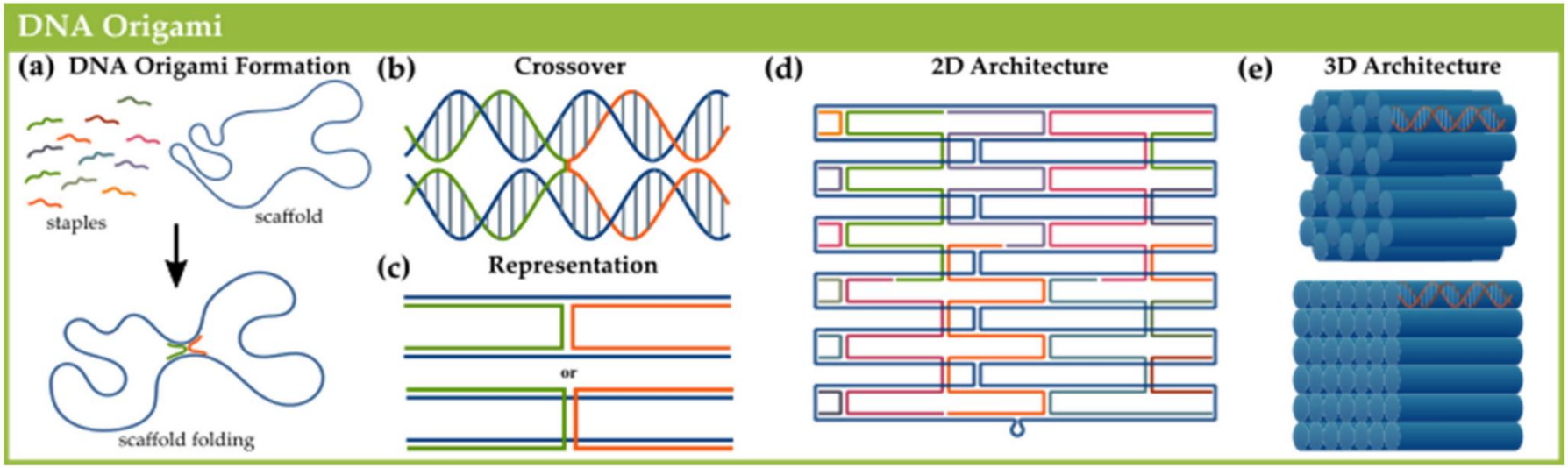


- DNA origamisi DNA molekülünü katlayarak istenilen şekilde nano boyutta yapılar oluşturur.

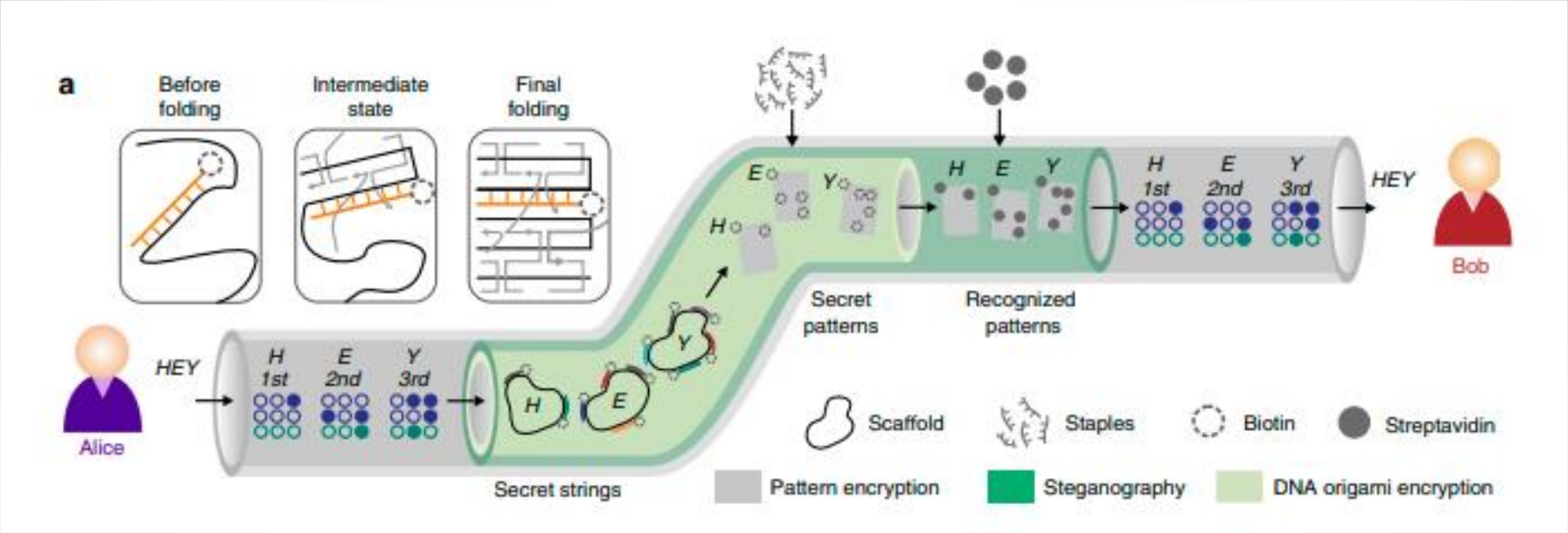


Bu yöntem farklı aşamalardan oluşur:

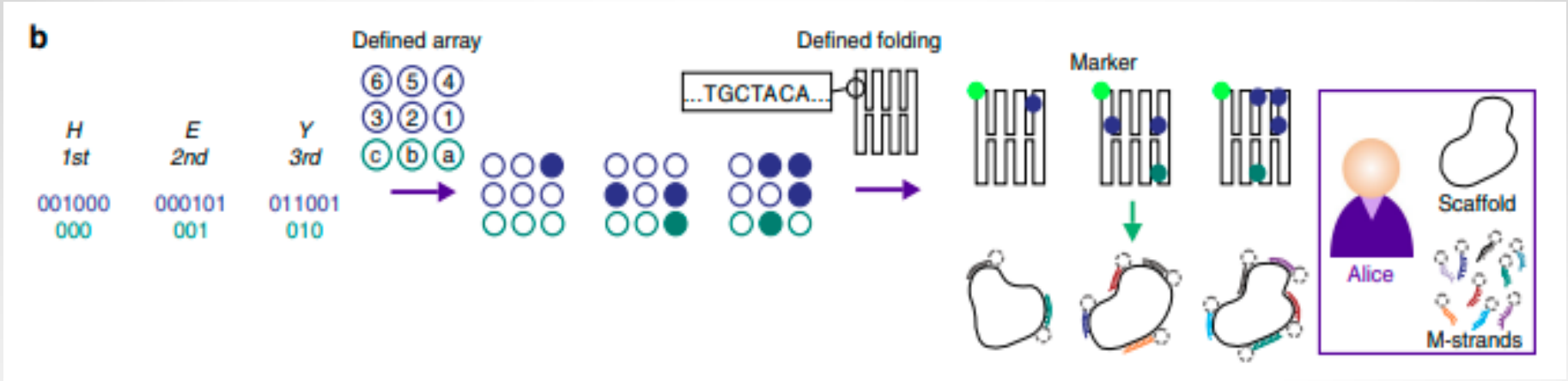
- İlk adımda tasarlanacak şekil (örneğin yuvarlak bir gülen yüz) seçilir.
- Daha sonra dikdörtgen şeklindeki DNA bloklarıyla belirlenen şekil oluşturulur.
- Sonraki aşamada uzun tekli bir DNA zinciri ikili sarmal yapıdaki DNA bloklarının üzerinden ileri ve geri katlanarak ilerler. Bu sırada DNA zincirleri arasında bağlantılar kurulur.
- Kısa DNA zincirleri kullanılarak, katlanan DNA zinciri sabitlenir.



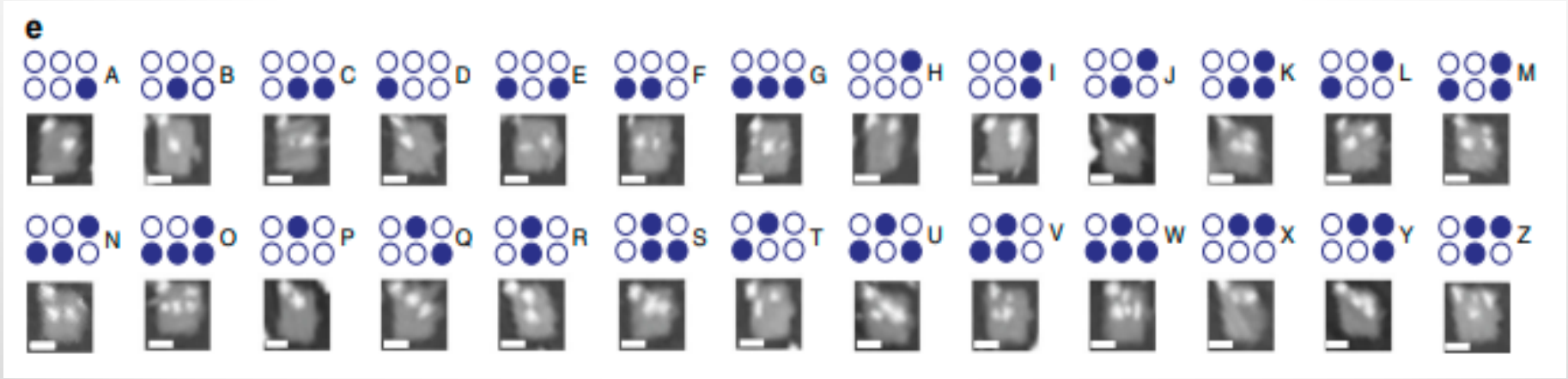
- 1999’da gizli mesajlar için DNA tabanlı bir steganografi şeması geliştirildi ve DNA kriptografisi çağı açıldı.
- Bununla birlikte, bu DNA tabanlı stratejiler **genellikle yalnızca dizi bilgisinden yararlanırken**, DNA'nın yapısal potansiyelini büyük ölçüde görmezden gelirler.

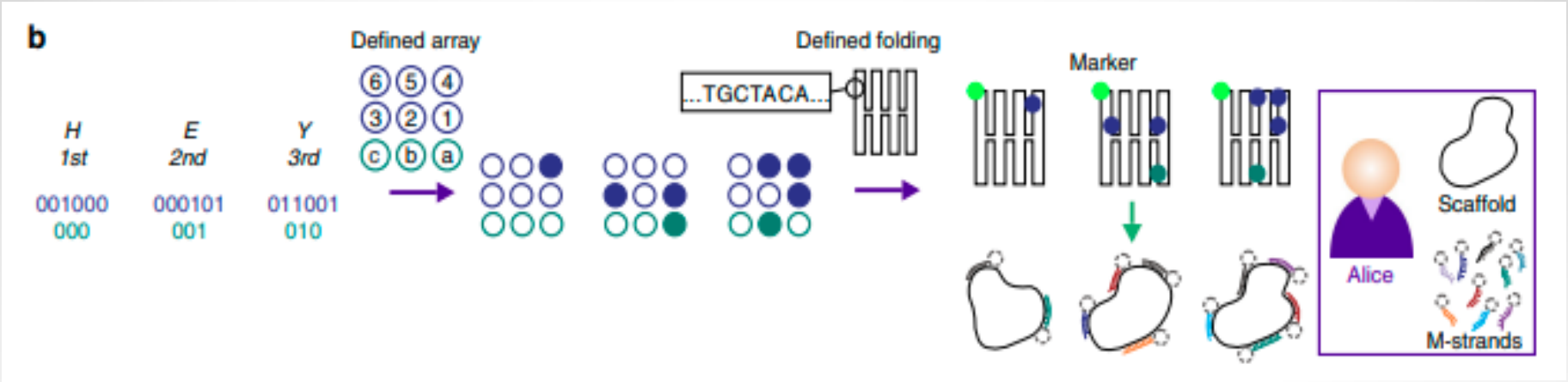


- Tüm süreç üç katmandan oluşur. Bunlar mesajın nokta düzeninde şifrelenmesi,(gri kısım) ardından bir steganografik ara katman(yeşil kısım)ve son olarak en içteki katman olarak iç içe kanalla temsil edilen DNA origami şifrelemesi (DOE)(soluk yeşil).

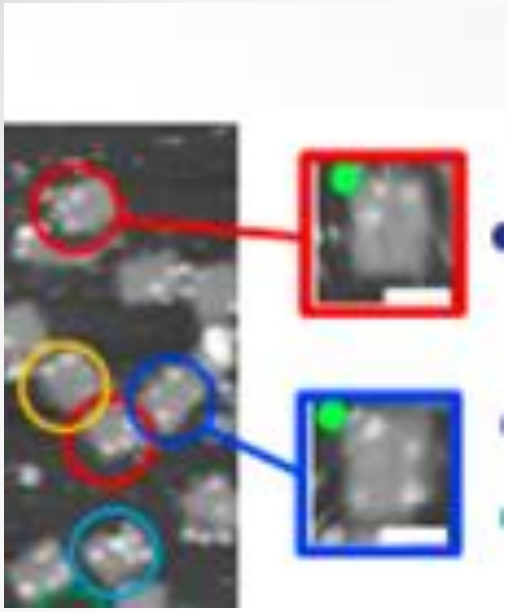


- Alice başlangıçta "HEY" düz metin mesajını harf harf ikili sayılara kodladı, ve mesajdaki her harfin ilgili konumlarını da şifreledi. Braille benzeri bir yapı oluşturdu.
- Modeldeki her nokta, harfleri veya konumlarını kodlayan ikili sayıların ayrı bir rakamını temsil eder..

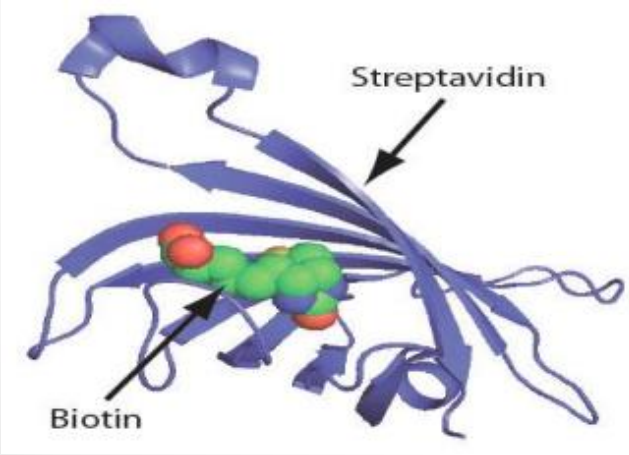


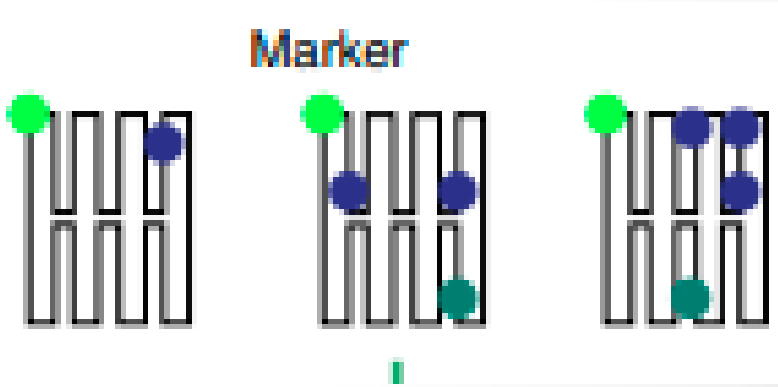


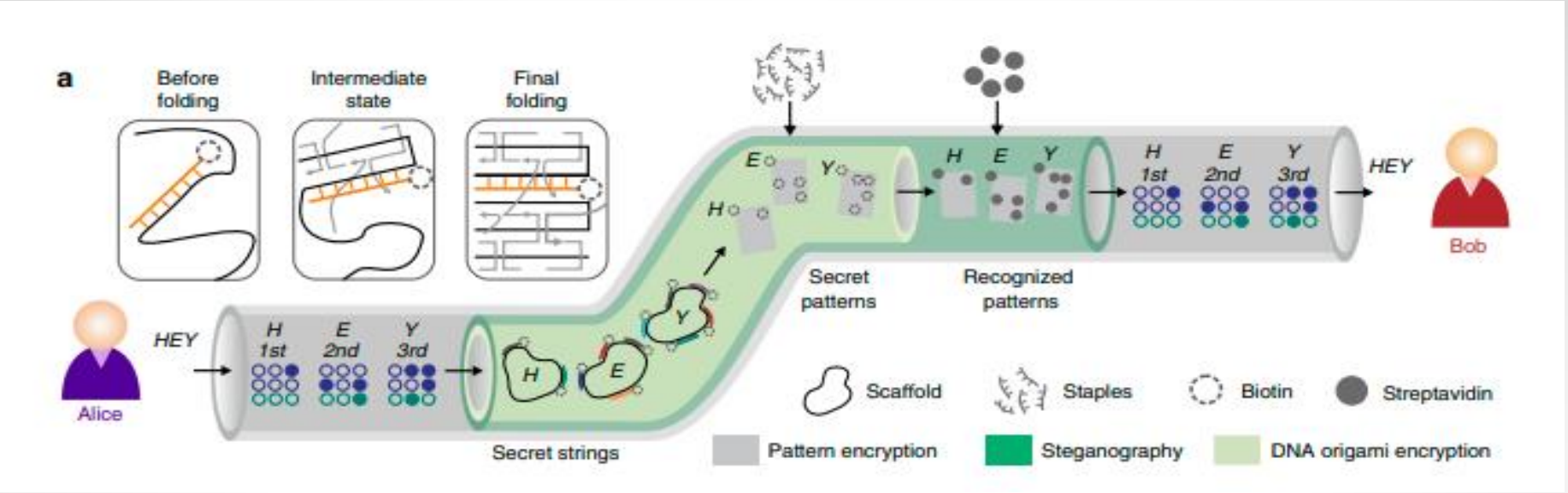
- Daha sonra bir sonraki şifreleme adımı için DNA origami katlanabilir şeması kullanıldı. Katlanabilir yani protein molekülünün üç boyutlu girift formunu alması anlamında kullanılıyor.
- Daha önemlisi origami yapısı bu aşamada DNA iplikçikleriyle fiziksel olarak üç boyutlu bir yapı oluşturmadı.
- Bunun yerine bir dizi biyotinlenmiş mesaj zinciri ("M-strands") yapı iskelesi iplikçiklerine hibritleştirildi.
- Biyotin, literatürde, H vitamini veya B7 vitamini olarak da adlandırılan bir vitamindir. Biyotin; moleküler biyoloji uygulamalarında önemli bir moleküldür. **Bunun en büyük sebebi ise, streptavidin için yüksek bağlanma eğilimi göstermesidir.**
- Streptavidin proteni ise bizim için burada şifreyi çözmek için gerekli.



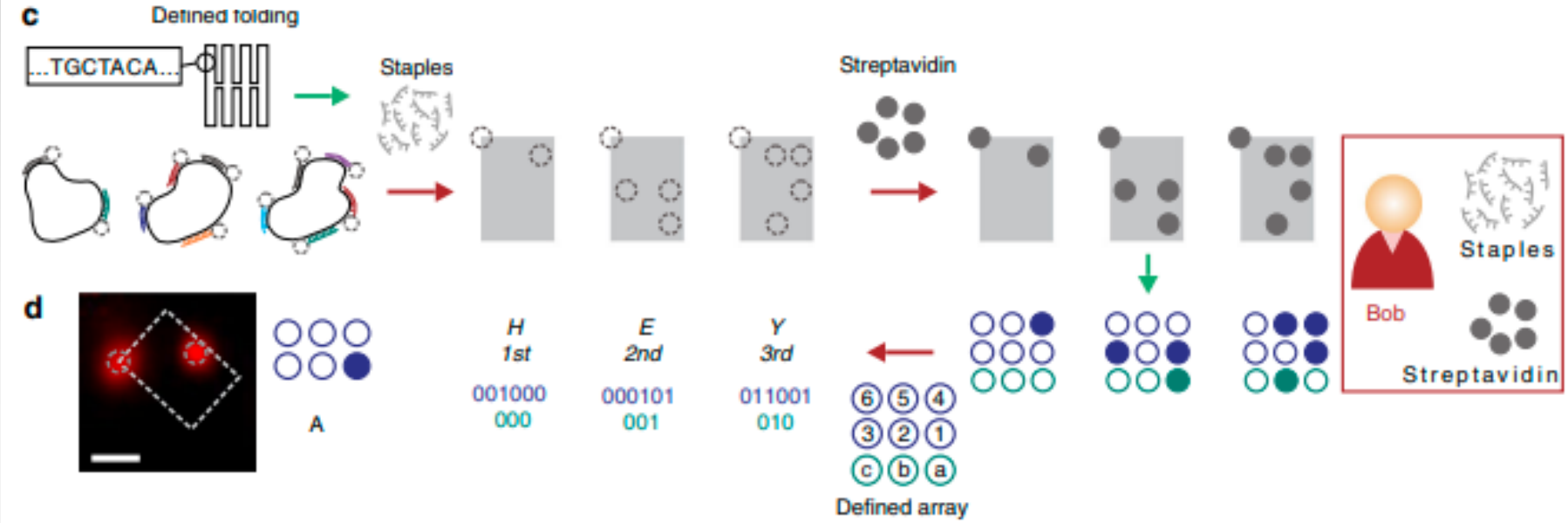
- Yapısal olarak simetrik bir DNA origamisi için, **modelin benzersiz bir şekilde tanımlanmasını kolaylaştırmak için** bir işaretleyici olarak ek bir M-strand(M-zinciri/dizisi) eklendi.



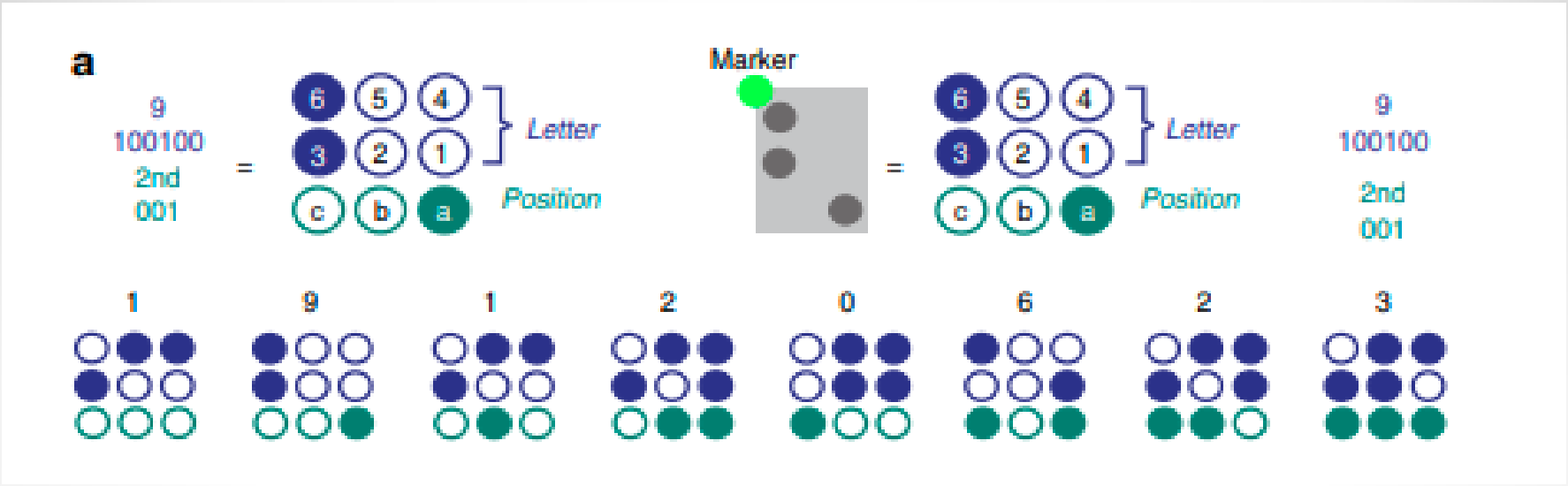




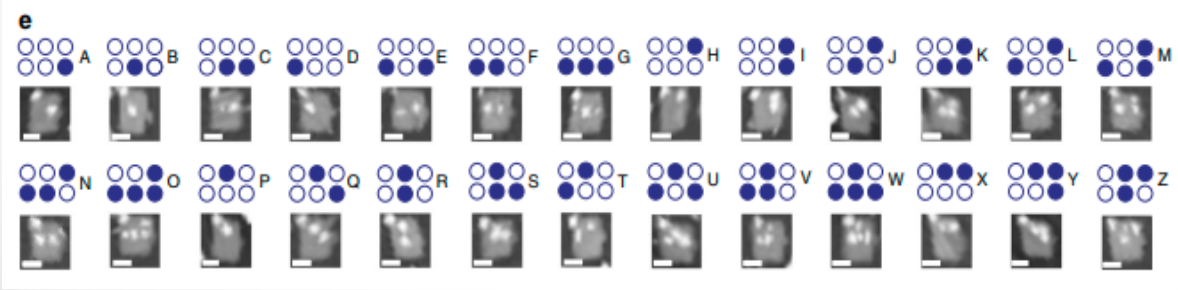
- Bu şekilde elde ettiğimiz noktalı yapı M-strands'ları taşıyan **yapıların bir kombinasyonu halinde şifrelenmiştir.**
- İlgili **anahtarımız** bu yapıların(scaffold) **tanımlanmış uzunlugu, sırası ve katlama şekli** ile spesifik olarak katlanması ile oluşturulur.
- Biyotinlenmiş durumlar potansiyel düşmanlar tarafından görülemez ve steganografi ile ek koruma sağlanır.

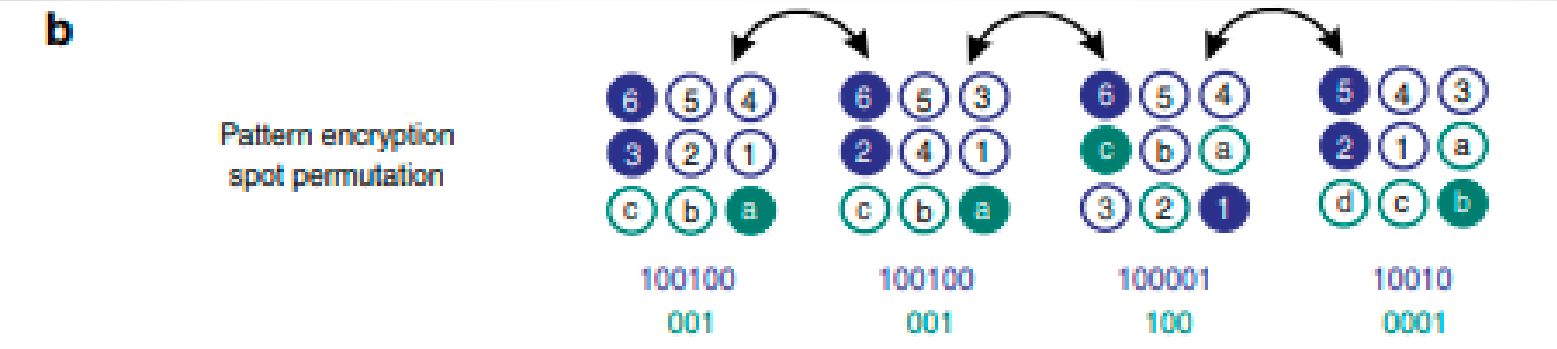


- Atomik kuvvet mikroskobu altında modelleri görünür hale getirmek için streptavidin ekledi.
- Son olarak, Bob streptavidin modellerinin şifresini tek tek çözerek model şifreleme için tanımlanan diziye dayalı olarak "HEY" düz metin mesajını elde etti.
- Alternatif olarak, stokastik optik rekonstrüksiyon mikroskobu (STORM) ile ortaya çıkarılabilen DNA modelini tanımlamak için **flüoresan etiketli M-strands kullanıldı.**

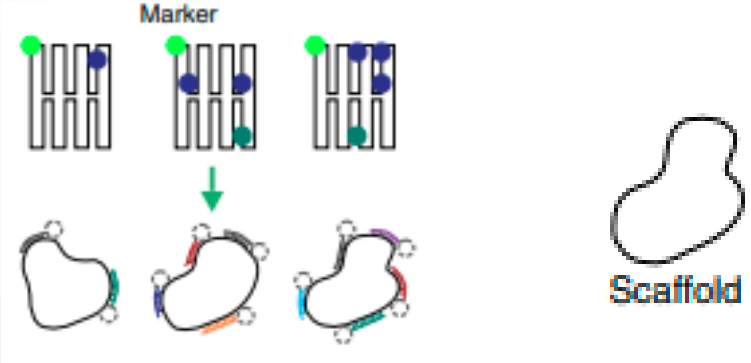


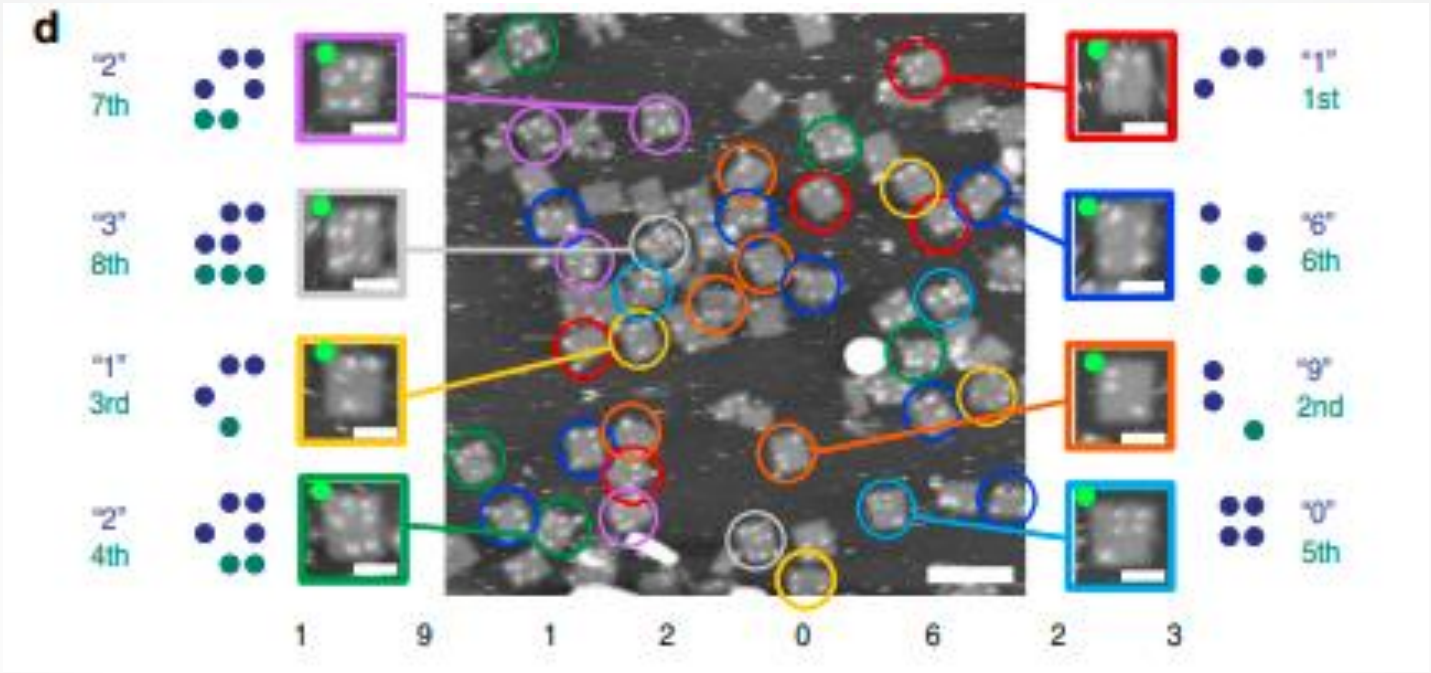
- Alan Turing'in doğum günü olan “19120623” mesajı şifrelenecektir.
- Örnek olarak “9” sayısı ve konumu “2” ayrı ayrı ikili sayılara dönüştürüldü ve bir nokta deseni ile gösterilir.





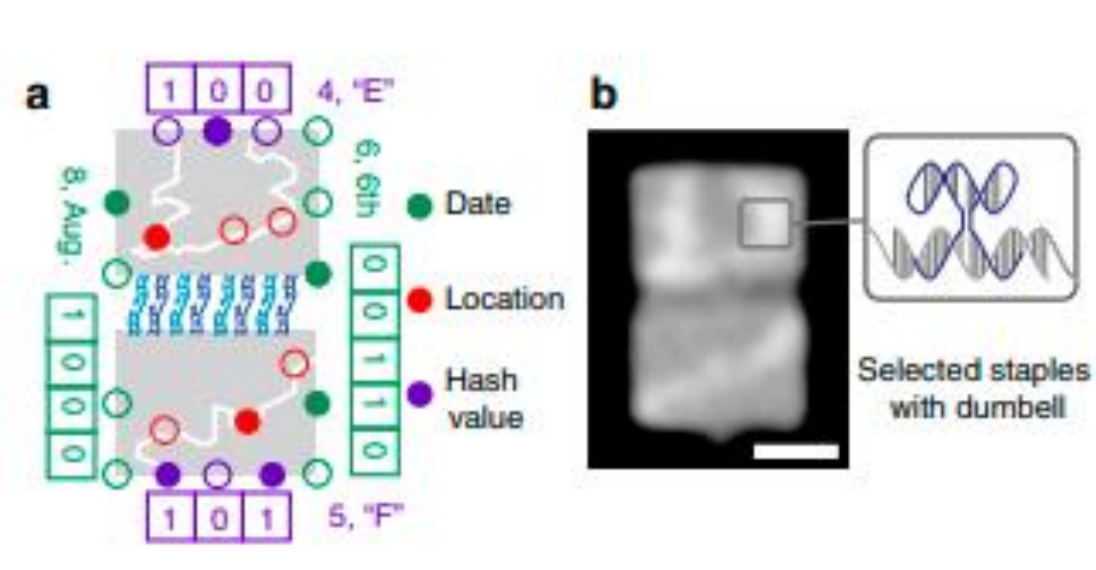
- Model şifreleme için anahtar uzayı, harfleri oluşturan binary sayılarla veya konumlarını temsil eden noktaların olası permütasyonlarının sayısından türetilir.
- Pratik olarak kaba kuvvet(brute-force) saldırısı mümkün değildir.
- Uygulamada, iletim sırasında DNA ortamının sahtesiyle değiştirme ihtimali oldukça düşüktür.



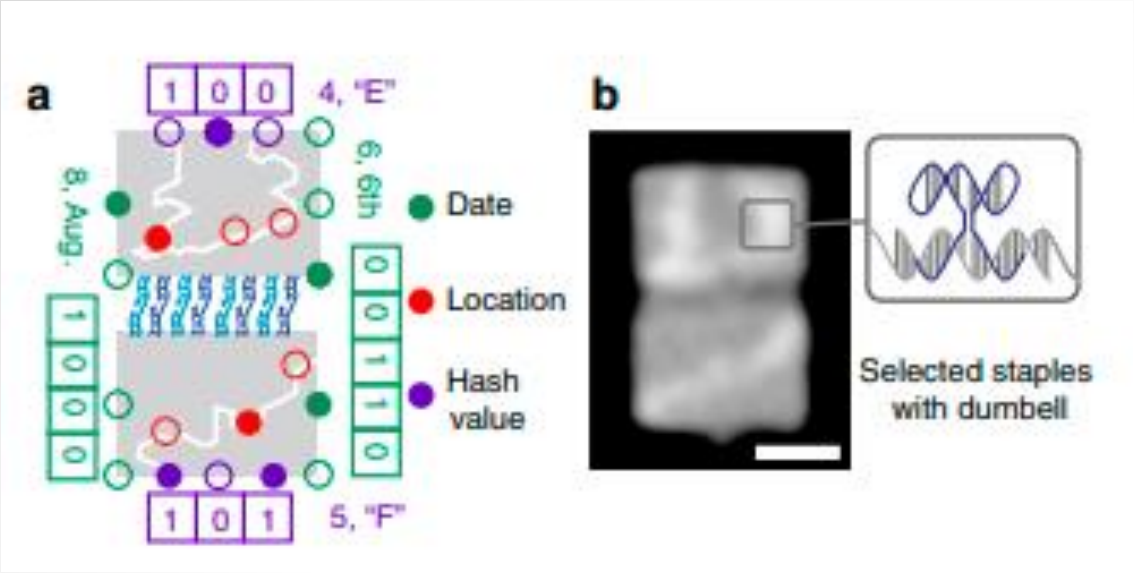


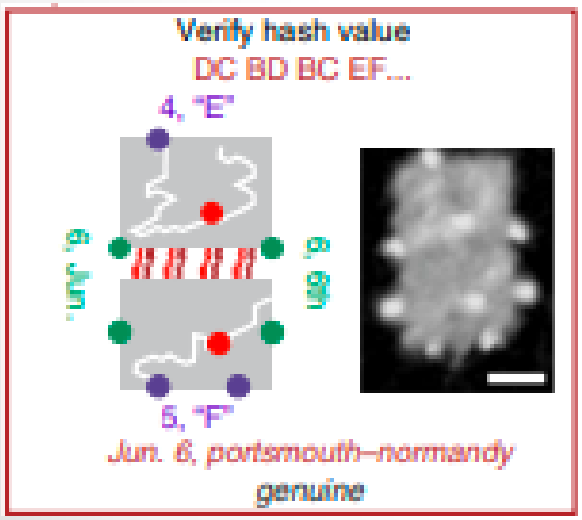
- Şifre çözmede sadece MARKER streptavidini taşıyan yapılar dikkate alınmıştır.
- MARKER ile her desen, konum numarasına göre tanındı.

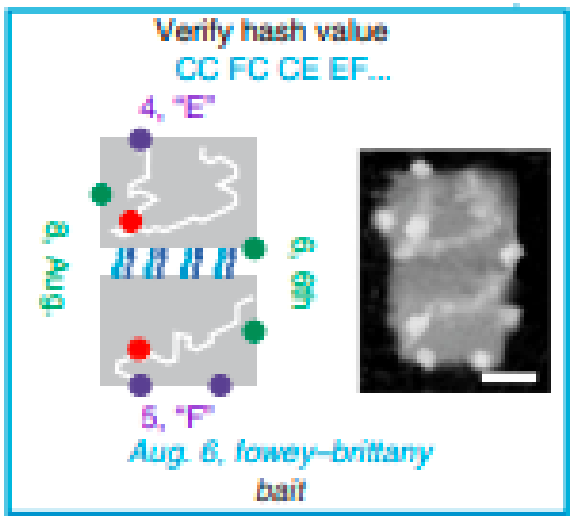
- DNA origamisi 'nin güvenlik seviyesini daha da artırmak amacıyla mesajların bütünlüğünü korumak için farklı DNA origami yapıları arasında özel tanıma etkileşimleri oluşturulmuş.
- Yani, farklı varlıkların kodlanmış bilgilere farklı erişimleri olacaktır.



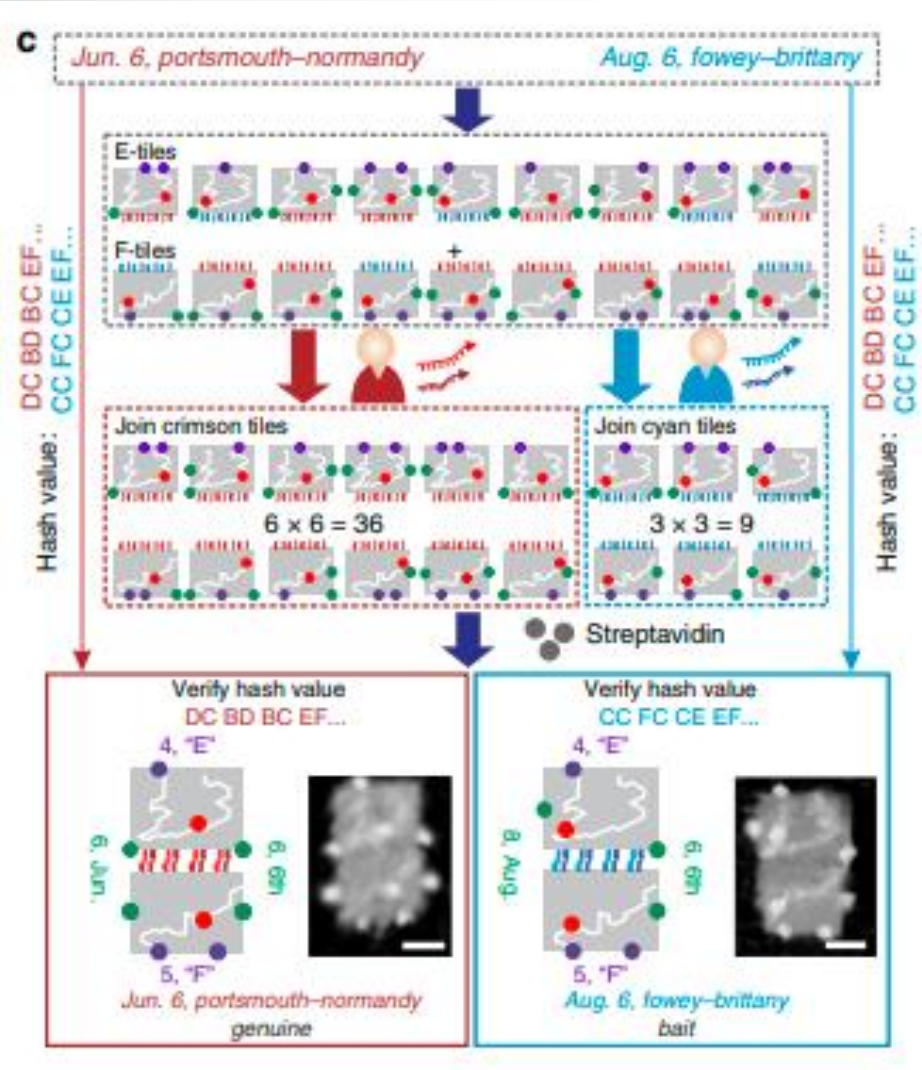
Örnek olarak, İkinci Dünya Savaşı sırasında Müttefik Kuvvetler tarafından gerçekleştirilen bir operasyonunun istihbaratı, Şekil a'da gösterildiği gibi bir nokta deseni ile temsil edilmektedir.



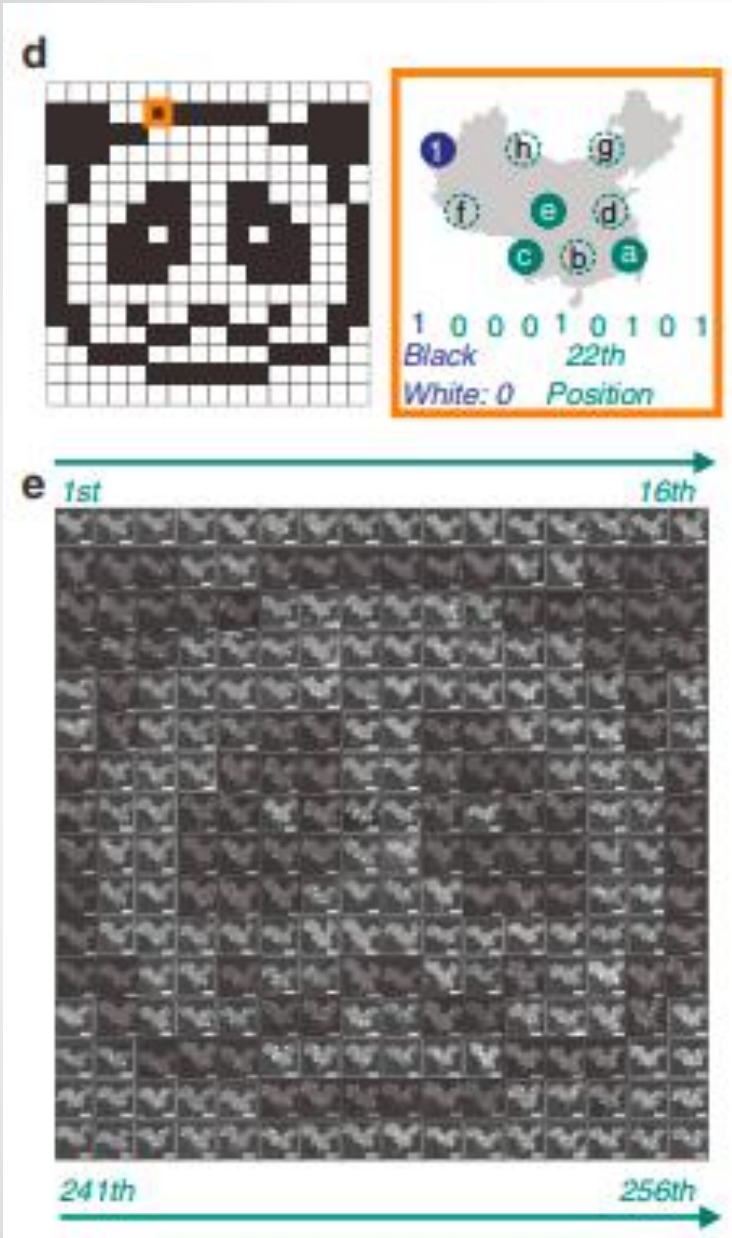




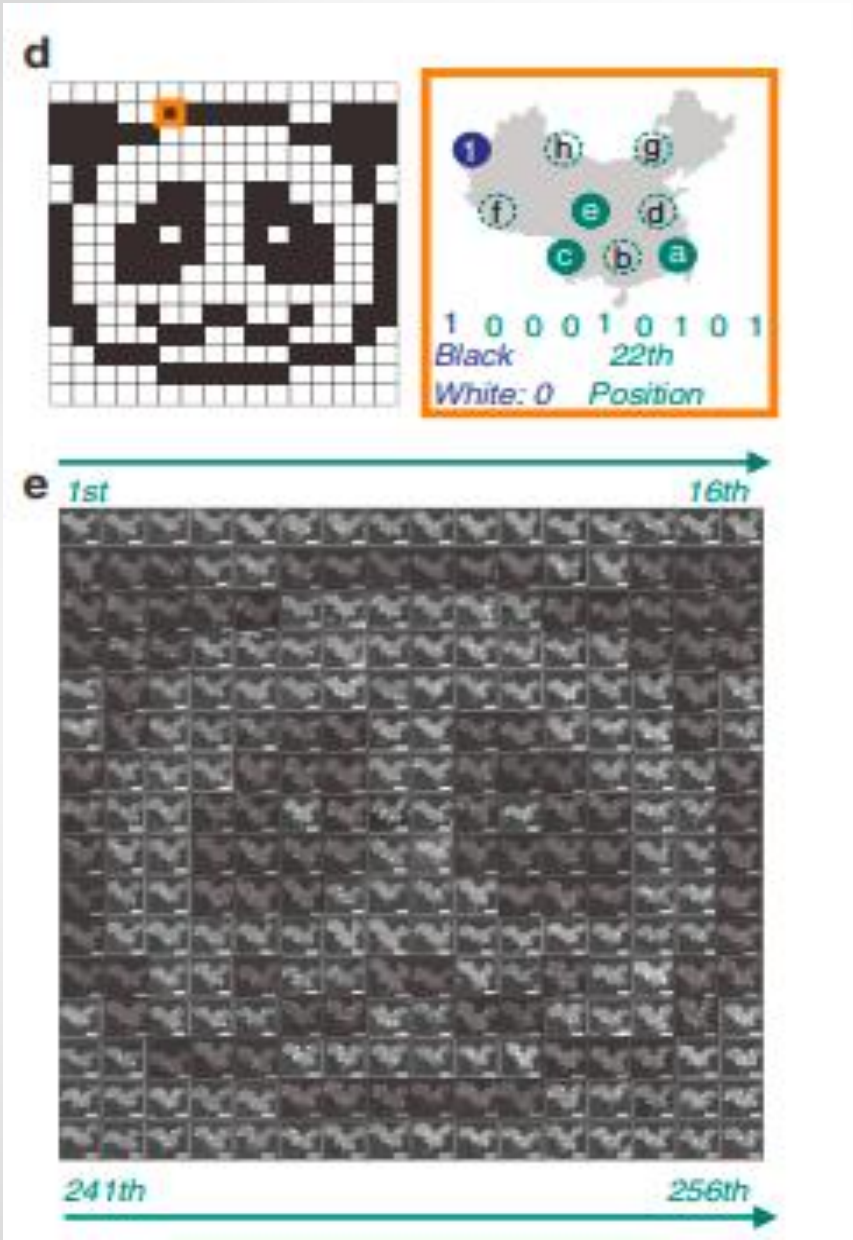
- Sırasıyla İngiltere veya Fransa'nın kıyı şeridinin bir haritası, farklı DNA origamilerinde, tasvir edilmiştir.
  - İlk olarak, birleştirilmiş mesaj "Jun. 6, Portsmouth-Normandiya; 6 Ağustos, Fowey-Brittany",
  - Mor noktalar, mesajın bütünlüğünü korumak için kullanılır. Doğrulama için.



- Mesajın sırasıyla Bob ve Mallory'ye gönderilen bölümlerine karşılık gelen orijinal hash değerleri, doğrulama için onlara dağıtıldı.
- Hash değerlerinin her ikisi de doğru olarak tanımlanır.
- Mallory'nin şifreleme için tüm anahtarları ele geçirdiğini varsayalım, Bob ile aynı biyotin desenleri kombinasyonunu elde edecektir.
- Bununla birlikte, Bob'un bağlayıcı şeritleri, gerçek mesajı taşıyan grubunu seçerken Mallory, yem mesajını taşıyan grubu seçer.
- **Sonuç olarak Bağlayıcı diziler, Bob ve Mallory'ye mesaja farklı erişim sağlamak için bir şifre görevi görür; bu, Bob'un gerçek mesaja erişimini sağlarken, Mallory bir yem mesajıyla kandırılır.**



- DNA origami şifrelemesi (DOC)'nin müzik notaları ve resimler gibi diğer veri formatlarının iletimi için de çok yönlü bir yöntemdir.
- Örneğin 256 bitlik bir panda görüntüsünün aktarımı yapılmış.
- Siyah ve beyaz olan pikseller binary sayılara çevrilir.
- Görüntünün pikselleri, 0'dan 255'e kadar artan konum numarası ile soldan sağa sıra sıra numaralandırılır.
- Görüntüyü iletmek için Çin'in dokuz noktalı bir desen taşıyan haritası DNA origami yapısı kullanıldı.
- Donanmada sol üst nokta rengi temsil etmek(0 veya 1)için kullanılırken diğer sekiz nokta pikselin konumunu temsil eder (toplamda 2^8 = 256 piksel).



Sol üst köşedeki nokta içinde siyah için 1 beyaz için 0 kullanılarak piksel bilgisi taşınır. Turuncu kutudaki desende pikselimizin siyah olduğunu anlıyoruz. Geriye kalan 8 nokta ise pikselin bize konumu veriyor. 00010101 ile konumun 22 piksel olduğunu bulmuş oluyoruz.

Şekil e, panda görüntüsünü oluşturan tüm 256 streptavidin modelini göstermektedir.

- Çalışma güvenli iletişim için mesajların DNA origamiyi tanıtan bir kriptografi yöntemini göstermektedir.
- DNA origami şifrelemesi ile mesajlar gizli braille benzeri kalıplara çevrildi (7249-nt M13mp18 iskelesi(Scaffold) kullanmak, 700 bitin üzerinde teorik bir anahtar boyutuna karşılık gelir).
- Protein bağlamaya dayalı steganografi ayrıca mesajın gizliliğini de garanti ediyor.
- Yaklaşımımızı pratik bir veri şifreleme tekniğine dönüştürmek için, kalıpları kodlamak için streptavidin yerine başka moleküler işaretleyiciler kullanılabilir.