



ASAL FAKTÖRLER

Klonlanamayan donanım (2)

ÇETİN KAYA KOÇ koc@sehir.edu.tr

Eşdeğer cihazların birbirlerinden farklılığı, bir anlamda onların randomize olması demek. Randomizasyon, bir cihaza kimlik atayıp onunla tekrar karşılaştığımızı tanımamızı sağlar, yani bir kimlik tanıma veya doğrulama metodudur. Bir önceki yazıda belirttiğim gibi, söz konusu randomizasyon iki türlü elde edilebiliyor: Ya dışardan bir şekilde ilave ederiz (explicitly introduced randomness) veya zaten cihazın doğasında var olan (intrinsic randomness) randomizasyonu ölçeriz.

Bu yazımın konusu cihaz doğasındaki randomizasyon.

Bütün eşdeğer cihazlar (örneğin, aynı model iPhone4 cihazları) eşdeğer bileşenlerden (ekran, kamera, hoparlör/mikrofon, flash hafıza, vs.) oluşuyor.

Bu bileşenler her ne kadar eşdeğer olsalar bile, aralarındaki üretim değişkenliği (manufacturing variability) dediğimiz minik farklılıkları barındırmak zorundadırlar. Örneğin, kamera sensör matrisi karesel bir şekilde organize edilmiş ışığa duyarlı birkaç milyon fotosel sensörden oluşur. Her bir fotoselin ışık şiddeti ve rengine duyarlılığı farklılıklar gösterir ve bu da bir sensör matrisini diğerinden dolayısıyla bir kamerayı diğerinden ayırır. Bu farklılıkları modelleyip, ölçmeyi başarabilirsek, bir kamerayı diğerinden ayırmayı da başardık demektir. Burada elde edeceğimiz eşdeğeri olmayan (unique) bir sayıyı kameramızın kimliği olarak kullanılabiliriz.

Bunun bize olağanüstü faydaları var: Bu kimlik sayısını kullanarak, o kameranın çektiği her resme bir kimlik atamak (watermarking) mümkün; üstelik bunu kameranın içinde, resim çekilir çekilmez bile başarabiliriz. Entelektüel sermaye veya sahipliği bundan daha etkin koruma yolu olamaz sanırım. iPhone, Android veya BlackBerry gibi akıllı telefonlara uygulanacak bu metotla, telefona kimlik atamamız ve ardından telefonu güvenli bir platforma dönüştürmemiz söz konusu. Birkaç yazı önce bahsettiğim Intryca Claveo teknolojisi işte bu anafikre dayanıyor. Telefonlara bu şekilde atanan ve eşdeğer cihazları birbirinden ayırdetmemizi sağlayan bu metodoloji, eninde sonunda akıllı telefonumuzu bir otantikasyon cihazı olarak da kullanmamıza olanak tanıyor.