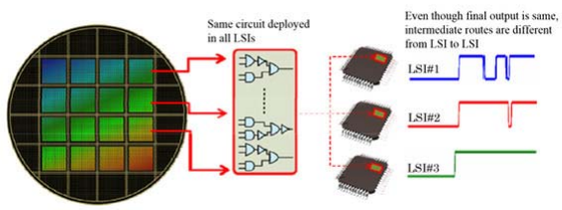
Mitsubishi Electric, Ritsumeikan Üniversitesi ve JST, IoT Cihazları için Güvenlik Çözümü Geliştirdiler

05.02.2015

LSI'ların bireysel farklılıklarını kullanarak gömülü cihazların güvenliğini ve emniyetini koruyor

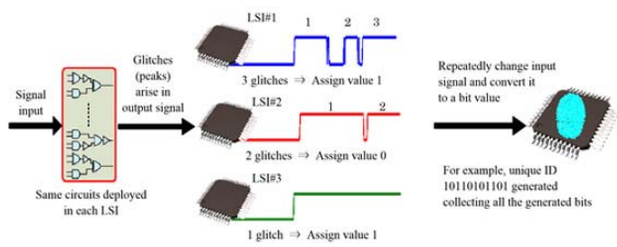
Mitsubishi Electric Corporation (TOKYO:6503), Ritsumeikan Üniversitesi ve Japonya Bilim ve Teknoloji Ajansı (JST), Nesnelerin İnternetinde (IoT) bağlantılı cihazlar için gizlilik ve doğrulamayı sağlamak üzere üretim sırasında ortaya çıkan büyük ölçekli entegrasyonların (LSI'lar) bireysel farklılıklarını kullanan bir güvenlik teknolojisi geliştirdiklerini açıkladılar. Yeni teknoloji, gömülü programları koruyarak ve yanıltıcı sinyalleri engelleyerek ağ tabanlı cihazlar için güvenlik risklerinin azaltılmasına yardımcı oluyor. Mitsubishi Electric, Nisan 2016'dan itibaren teknolojiyi ürünlerinde uygulamaya başlayacak.

LSI'lar, çıkış değerini dikte eden dahili devrelere dayalı hesaplamalar yaptığı için aynı devrelere sahip LSI'lar aynı giriş değerini işlerken aynı sonuçları veriyor. Ancak hesaplama sonucuna götüren ara yollar, her bir LSI'da farklı olup, yeni teknolojide aynı devrelere sahip LSI'lar için özel birer tanıtım numarası (ID'ler) oluşturmak için kullanılan birer parmak izi olarak görev yapıyor. Özel ID, LSI paketi açıldığında ve içi incelendiğinde dahi analiz edilemiyor. Çünkü ID yalnızca devre çalışırken beliriyor. Yalnızca belirlenen ID'ye sahip LSI'nın bulunduğu cihazda şifresinin çözülmesi ve kullanılması için gömülü program şifreleniyor. Ayrıca cihazlar, yalnızca belirlenen ID'lere sahip cihazlara bağlantıyı mümkün kılmak üzere konfigüre edilebiliyor.

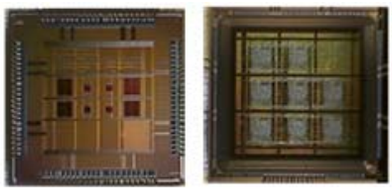


Şekil 1: Farklı LSI'larda devre geçitlerinin hesaplama süreçlerinde küçük farklılıklar

Özel ID aşağıdaki şekilde oluşturuluyor:
Aşama 1. Sinyal girişinde ortaya çıkan küçük arızaları (pikleri) sayın. Eğer çift sayıysa, çıkış biti 0; tek sayıysa, 1 olacaktır. **Aşama 2.** Sinyal girişini tekrar tekrar değiştirin ve karşılık gelen çıkış bitini hesaplayarak özel bir ID oluşturun.



Üç fonksiyon—özel ID oluşturma, şifreleme ve doğrulama—unsurlarının bir kısmının paylaşılmasına izin vermek suretiyle küçük bir devre alanında uygulanabiliyor. Gerekli alan, her bir fonksiyonun ayrı ayrı uygulandığı durumlarda üçte bir oranına düşüyor. Ayrıca, çoklu üretim proseslerinin kullanılması suretiyle Ritsumeikan Üniversitesi ile ortaklaşa geliştirilen LSI prototiplerinin özel ID'leri istikrarlı bir şekilde oluşturduğu teyit edildi. Bu sayede teknoloji modülerleştirilebiliyor ve genel LSI tasarım akışında kolaylıkla uygulanabiliyor.



Şekil 2: Sinyal geçişiyle benzersiz ID'ler oluşturan LSI prototipleri (Sol: 65 nm, 2.1 mm2; Sağ: 180 nm, 2.5 mm2)

Ağ tabanlı gömülü cihazların kullanımı artarken, program analizi, sahtecilik, veri hırsızlığı ve cihaz yanıltıcı sinyallerini önlemeye yönelik karşı tedbirler giderek daha fazla önem kazanıyor. Özellikle yüksek güvenlik gerekliliği içeren gömülü cihazlarda, program ve veri korumaya yönelik tam tedbirlere ihtiyaç duyuluyor. Genel olarak, kriptografik kullanıma yönelik ID bilgileri cihaza gömülü hafızada depolanıyor ve bu bilgiler cihazın kapatılmasından sonra da hafızada kalıyor. Bu nedenle LSI paketini açmak ve içindekileri incelemek