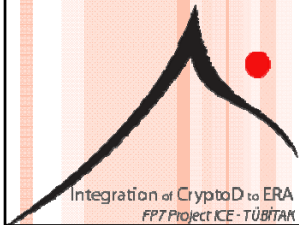


TEMEL RFID ETİKETLERİ



TASLAK

- Privacy
 - Killing and sleeping
 - The renaming approach
 - The proxying approach
 - Distance measurement
 - Blocking
 - Legislation
- Authentication
- The problem of PIN distribution



RFID ETIKETLER

- EPC etiketleri binli sayılarda mantık kapılarına sahip
- Bunların büyük bir kısmı temel haberleşme işlevleri için kullanılıyor
- Ancak yüzlü sayıda kapı güvenlik için ayrılabiliyor
- Gelişen teknolojiyle bu sayı artacak, güvenlik açısından daha çok işlev kazandırılacak



A - PRIVACY (MAHREMIYET)

6 çeşit yaklaşım vardır:

- Killing and Sleeping
- The renaming approach
- The proxying approach
- Distance measurement
- Blocking
- Legislation



1 - KILLING AND SLEEPING

- “Killing” işlemi bir okuyucu tarafından bir etikete verilen “KILL” komutu ile etiketin işlevsiz hale getirilmesidir
- “Killing” işleminin geri dönüşümü yoktur
- Kötüye kullanılmasını engellemek için PIN koruması yapılmıştır
- Böylelikle, yalnızca PIN’i bilen okuyucular söz konusu etiketi işlevsiz hale getirebilir



1 - KILLING AND SLEEPING

Dezavantajları:

- “Killing” işlemi tek yönlü olduğundan işlevsiz hale getirilen bir etiketın tekrar kullanılması olanaksızdır
- Geri dönüşümü olan uygulamalarda bu işlem kullanışsızdır
- Örnek: Kütüphaneler, eşya kiralayan dükkanlar
- Bunun yerine “sleeping” işlemi önerilebilir



1 - KILLING AND SLEEPING

- “Sleeping” işlemi bir okuyucu tarafından bir etikete verilen “SLEEP” komutu ile etiketin geçici olarak işlevsiz hale getirilmesidir
- Diğerinde olduğu gibi bu işlem de PIN korumalıdır ve belli okuyucular etiketi “sleep” moduna geçirebilir
- Aynı PIN ile söz konusu etiket “wake” moduna geçirebilir



1 - KILLING AND SLEEPING

Dezavantajları:

- Her etikete ait bir SLEEP/WAKE PIN'i bu işlevleri gerçekleştirebilecek okuyucu sahibi tarafından ezberlenmelidir
- Alternatif olarak okuyucunun etikete direk teması ile bu işlemlerin gerçekleşebilmesidir ki bu da RFID'nin en önemli özelliği, kablosuz haberleşmenin, göz ardı edildiği anlamına gelir



2 – THE RENAMING APPROACH

- Etikete özel olan kimliğin şifreli bir şekilde dışarıya söylenmesi mahremiyeti tam anlamıyla sağlamaz
- Etiket sürekli aynı bilgiyi dışarı verdiği için izlenebilirlik özelliği düşman tarafından kullanılabilir
- Bu durumda etiketin belli aralıklarla kimliğini değiştirmesi gerekmektedir



2-A - RELABELING

- Sarma, Weis ve Engels (SWE) etiketlerin unique kimliklerinin yok edilebileceğini, product-type kimliklerin ise daha sonrası için saklanabileceğini önermiştir
- Inoue ve Yasuura (IY) tüketicilerin etiketlere yeni kimlik verebilmelerini ve geri dönüşüm söz konusu olduğunda eskisini aktifleştirebilmelerini önermiştir



2-A - RELABELING

- (IY) ayrıca (SWE)'nin fikirlerini destekleyecek şekilde unique kimlik ile product-type kimliğin ayrı tutulmasını iki ayrı etiketle yapılabileceğini önermiştir
- Karjoth ve Moskowitz kullanıcıların etiketlerin bilgi yayılımını sınırlayabileceğini söylemiştir
- Good ve diğerleri kütüphanelerde kitap ödünç alımlarında etiketlere rastgele kimlik verilmesini önermişlerdir



2-A - RELABELING

Yorumlar:

- Unique kimliklerin yok edilmesi izlenebilirlik problemini de gizli sayım problemini de çözmüyor
- Rastgele kimlik kullanımı unique kimliğin saklanmasına yardımcı oluyor fakat izlenebilirlik problemini çözmüyor
- İzlenebilirlik probleminin çözümü kimliğin sıkça değişiminden geçiyor



INOUE VE YASUURA

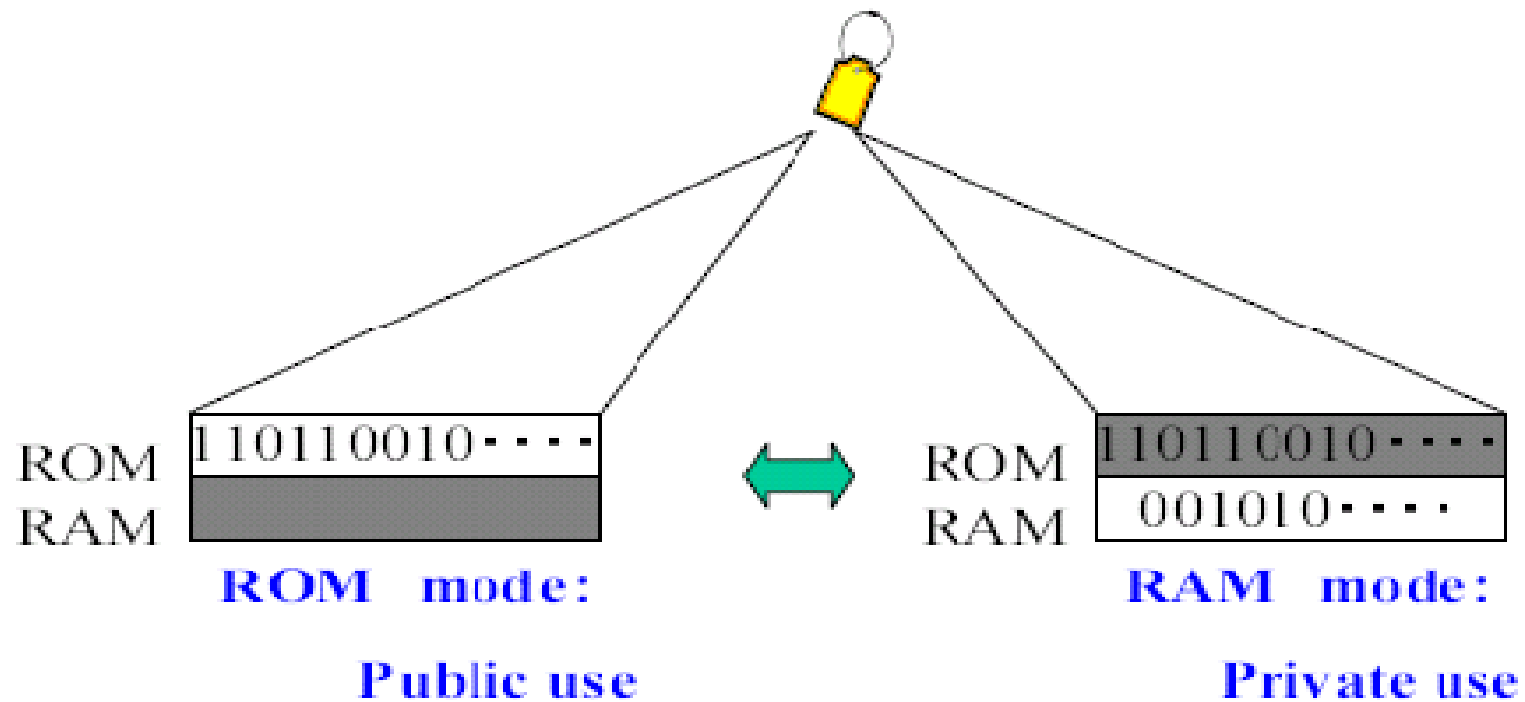


Figure 3: Restriction of identification to limited users



INOUE VE YASUURA

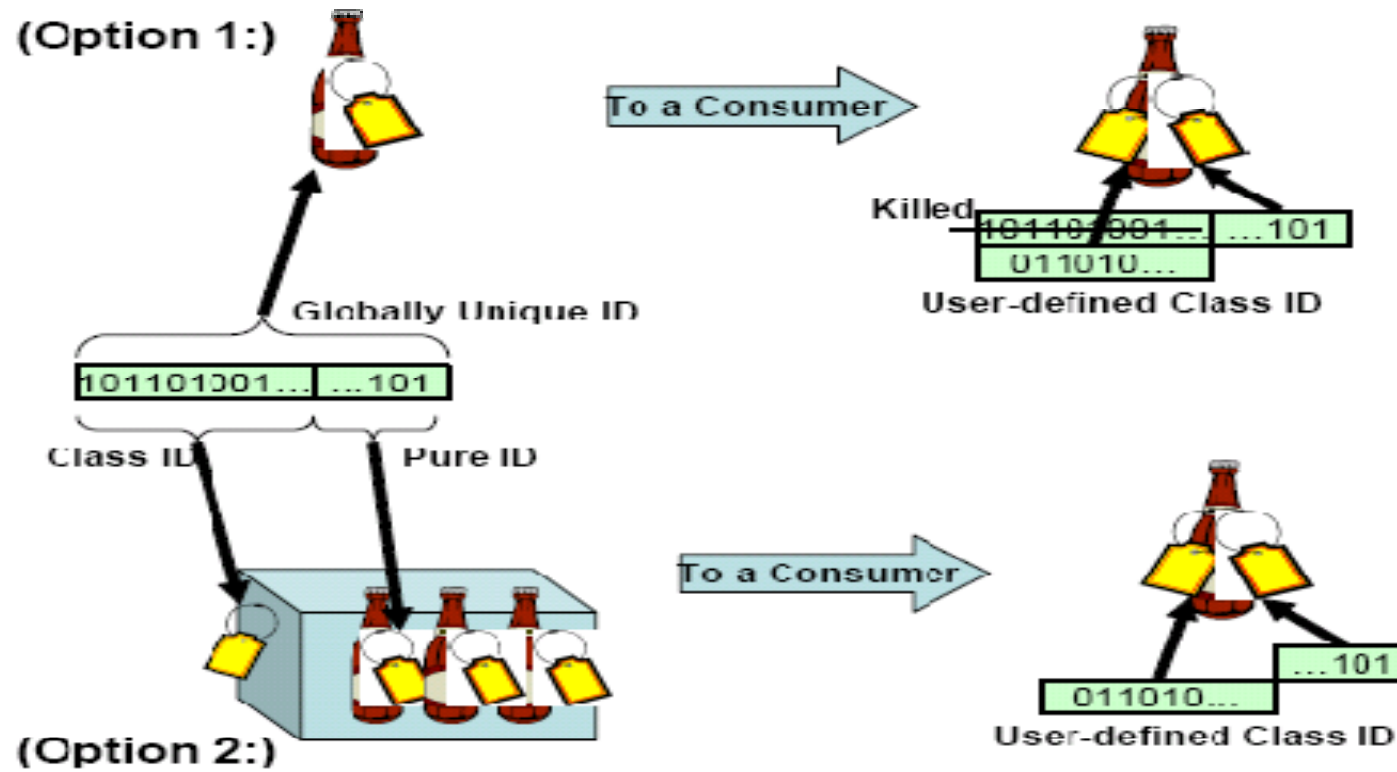


Figure 4: Physical separation of IDs



KARJOTH VE MOSKOWITZ

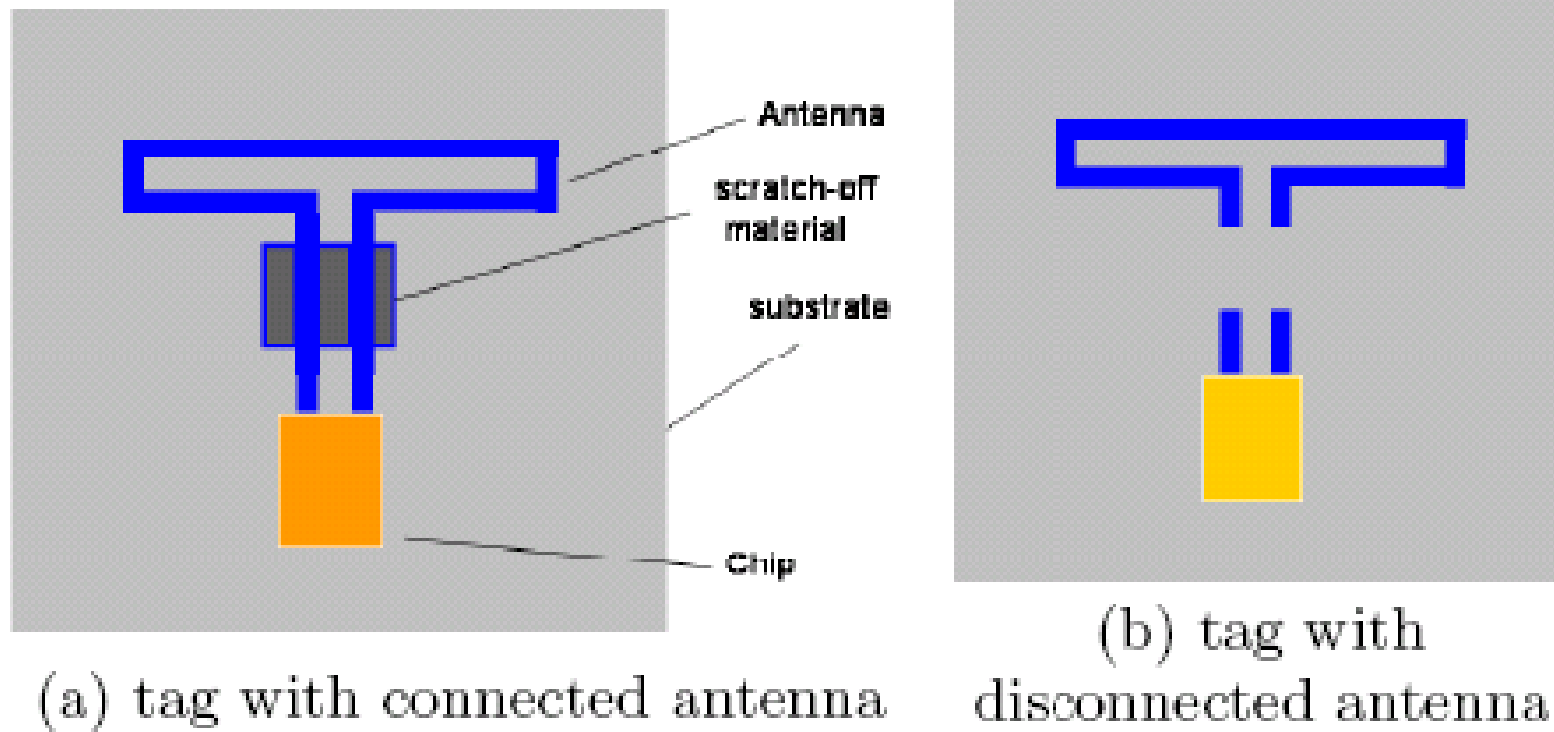


Figure 1: RFID tags with removable electrical conductor

KARJOTH VE MOSKOWITZ

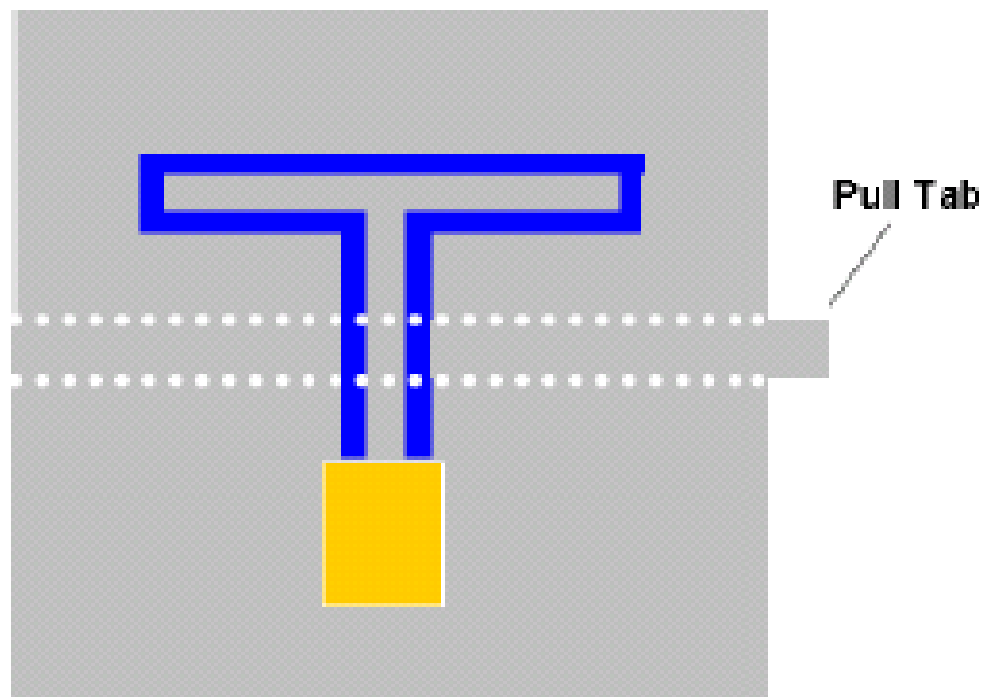


Figure 2: RFID tags with perforation



KARJOTH VE MOSKOWITZ

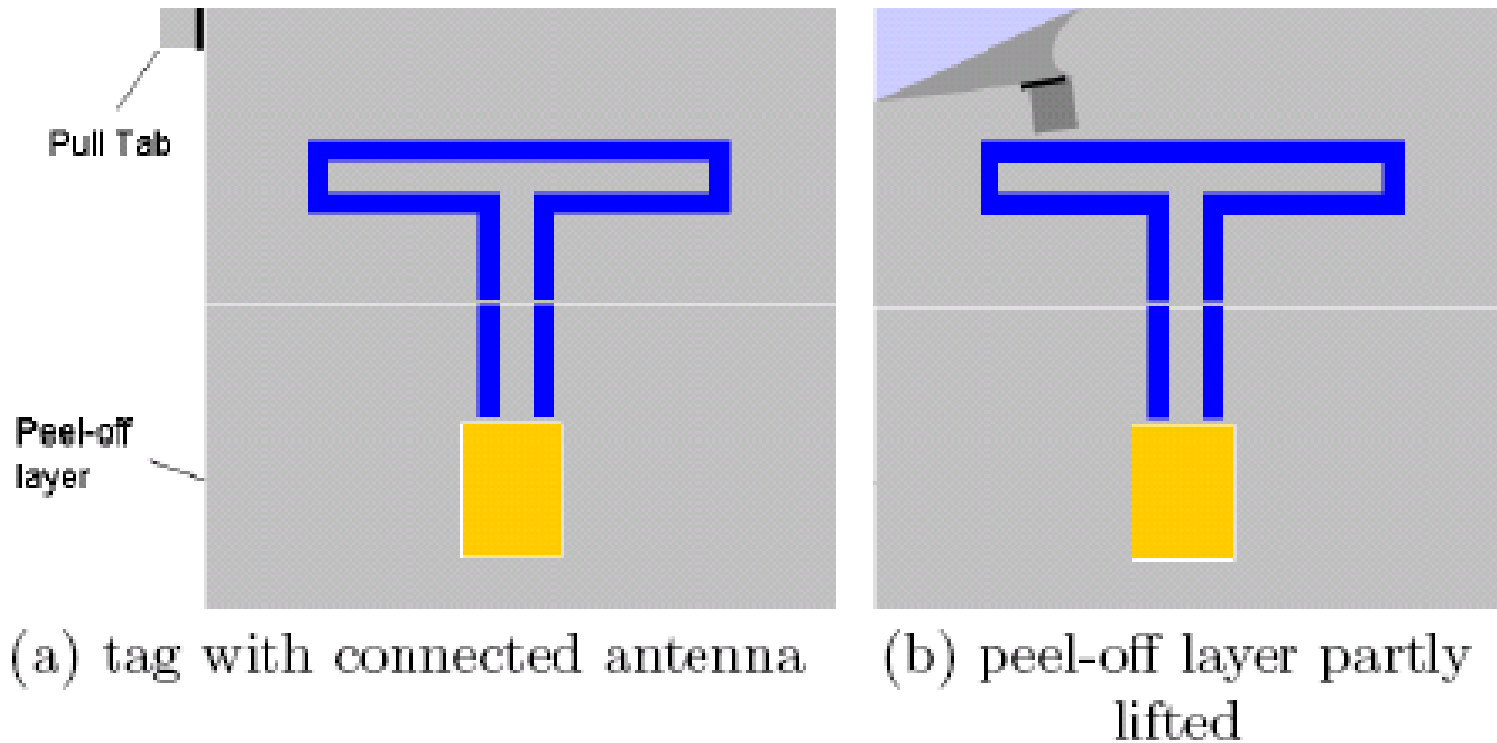


Figure 3: RFID tags with a peel-off layer



2-B – MINIMALIST CRYPTOGRAPHY

- Juels'a göre her etiket'in belli sayıda pseudonym'ları vardır
- Her sorgulamada okuyucuya birini söyler
- Yetkili okuyucuda bu pseudonym'lar vardır ve böylelikle etiketi tanıyabilir
- Etiket yetkili olmayan bir okuyucu tarafından sorgulandığında bütün pseudonym'ları öğrenmesini önlemek için cevapları yavaş vermeye başlar
- Yetkili okuyucuların pseudonym'ları güncelleme hakkı da vardır



THET C

Tag

$d \leftarrow (c \bmod k) + 1$

$c \leftarrow c + 1$

$\alpha' \leftarrow \alpha_d$

$\xrightarrow{\alpha'}$

if $\beta' \neq \beta_d$ then

output("reject") and abort

$\gamma' \leftarrow \gamma_d$

$\xleftarrow{\beta'}$

$\xrightarrow{\gamma'}$

$\xleftarrow{\tilde{\Delta}_{AEC}}$

$\{\text{update}(\Delta_\kappa, \tilde{\Delta}_\kappa)\}_{\kappa \in ABC}$

$\{\kappa \leftarrow \text{pad}(\kappa, \Delta_\kappa)\}_{\kappa \in ABC}$

Verifier

if α' is valid α_i for some tag T_x then

$tag \leftarrow x$

$\beta' \leftarrow \beta_i$

$\gamma \leftarrow \gamma_i$

mark α_i as invalid for T_x

else

output("reject") and abort

if $\gamma' \neq \gamma$ or $\gamma' = \perp$ then

output("reject") and abort

$\tilde{\Delta}_{ABC} \in_R \{\{0, 1\}^l\}^{3km}$

output(tag , "accept")

$\{\text{update}(\Delta_\kappa, \tilde{\Delta}_\kappa)\}_{\kappa \in ABC}$

$\{\kappa \leftarrow \text{pad}(\kappa, \Delta_\kappa)\}_{\kappa \in ABC}$

2-C – RE-ENCRYPTION

- Juels ve Pappu (JP) RFID bulunduran banknotlar üzerinde açık anahtarlı kriptografik sistem tasarlamışlar
- Banknotlar banknot seri numarası S'in PK açık anahtarıyla şifrelenmiş hali olan C'yi dışarı verir
- Yalnızca "law enforcement agency" SK gizli anahtarına sahip olarak C'den S'ye ulaşabilir



2-C – RE-ENCRYPTION

- ▶ İzlenme problemini çözmek için dükkanlar ve bankalar C 'yi PK kullanarak yeniden şifreleyebilmeli ve bu şifreleme sırasında S 'yi kaybetmemeliler (ElGamal)
- ▶ Yetkisiz okuyucuların bu şifrelemeyi yapamaması için banknotlar yazmaya erişimli optik anahtarlar içermeli ve ancak yetkili okuyucular bu anahtara sahip olmalı
- ▶ Güvenlik yeniden şifrelemeye dayandığından bu yöntem kullanışsızdır; ancak etikette kriptografik algoritmalar olmadan da güvenliğin sağlanabileceği gösterilmiştir



2-D – UNIVERSAL RE-ENCRYPTION

- Golle ve diğerleri genel RFID sistemleri için (SKi,PKi) ikililerini içeren bir açık anahtar alt yapısı önermiştir
- Bu sisteme göre C'yi tekrar şifrelemek için bir önceki şifrelemede hangi PKi kullanıldığı önemli değildir
- Golle'nin sisteminde herhangi bir şifreli C metni alakasız bir C' metniyle değiştirilebileceğinden ve tamamen farklı bir S metninin bulunmasına yol açacağından bütünlük problemi vardır



2-D – UNIVERSAL RE-ENCRYPTION

- Ateniese, Camenisch ve Medeiros bu sorunun her şifreli metnin merkezi bir otoritenin imzalaması yoluyla çözüleceğini ileri sürdüler, böylelikle herhangi bir şifreli metnin gerçek olup olmadığı doğrulama yoluyla anlaşılabilir
- Buna rağmen bu sistem (swapping) değiş-tokuş saldırısına dayanıksızdır, yani, iki tane doğrulanabilir şifreli metin kolaylıkla yer değiştirebilir



3 – THE PROXYING APPROACH

- RFID okuyucularının mahremiyeti koruması yerine tüketiciler bu işlevi gerçekleştiren aletler taşıyabilirler, örneğin; cep telefonları
- Floerkemeier, Schneider ve Langheinrich “Watchdog Tag” adında, çevredeki okuyucuları bulup onlar hakkında bilgi toplayan denetleme sistemini önermişler



3 – THE PROXYING APPROACH

- Juels, Syverson ve Bailey “RFID Enhancer Proxy” ve Rieback, Crispo ve Tanenbaum “RFID Guardian” adlı aletleri öne sürmüşlerdir
- “RFID Guardian” okuyucu isteklerini etiketlere iletir, yüksek güce sahip olduğundan birçok gelişmiş protokolü uygulayabildiği gibi GPS ve internet gibi farklı kanallardan da yardım alabilir



4 – DISTANCE MEASUREMENT

- Fishkin, Roy ve Jiang bir okuyucu sinyalinin sahip olduđu S/N'in, bu okuyucu ile etiket arasındaki mesafenin tahmini hesaplanmasında yardımcı olduğunu öne sürmüşlerdir
- Etiket çok basit bir devre yardımıyla bu uzaklığı kabaca hesaplayabilir ve dolayısıyla uzaklığa göre bir protokol tasarlanabilir
- Örnek; okuyucu uzaksa sadece product-type kimlik etiket tarafından açığa çıkarılırken, yakınsa unique kimlik de açığa çıkarılabilir



FISHKIN, ROY VE JIANG

- Triangulation via time-of-arrival analysis:
 - Etiketler kümesi ellerine geçen sinyalleri karşılaştırırlar ve mesafeyi kabaca bulurlar
 - Minimum maliyet ve altyapı ihlal edilir
 - RF dalgasındaki deęişimler yanlış hesaplamalara neden olur
- Triangulation via signal strength analysis:
 - Eline geçen sinyalin enerjisini normalde geçmesi gerekenle karşılaştırır ve mesafeyi kabaca bulur
 - Okuyucunun ne kadar enerji yolladığı bilinemez
 - RFID enerji alanı kurlsız ve yerel deęişimlerle dolu olduğundan doğru bir hesaplama yapılamaz



FISHKIN, ROY VE JIANG

○ Noise analysis:

- Etiket in eline geçen sinyalde gürültü ve sinyal enerjileri arasındaki ilişki mesafe hakkında bilgi verir
- Yakındaki bir okuyucu sinyale gürültü ekleyip etikete uzaktaymış gibi algıtabilir, ancak bu istenmeyen bir durumdur, tersi ise geçersizdir

○ Tiered revelation:

- Verici alıcının iyi niyeti oranınca elindeki bilgilerini paylaşır
- İyi niyet, paylaşılan kriptografik gizler de olabilir, okuyucu ile etiket arasındaki mesafe de olabilir



5 – BLOCKING

- Juels, Rivest ve Szydlo (JRS) etiketlerde “privacy bit” olmasına dayanan bir sistem önermişler
- “privacy bit”i 0 olan etiketler bütün okuyucular tarafından okunabilir
- “privacy bit”i 1 olan etiketleri ise hiçbir okuyucu okuyamaz, yani “privacy bit”i 1 olan etiketler “privacy zone”dadır



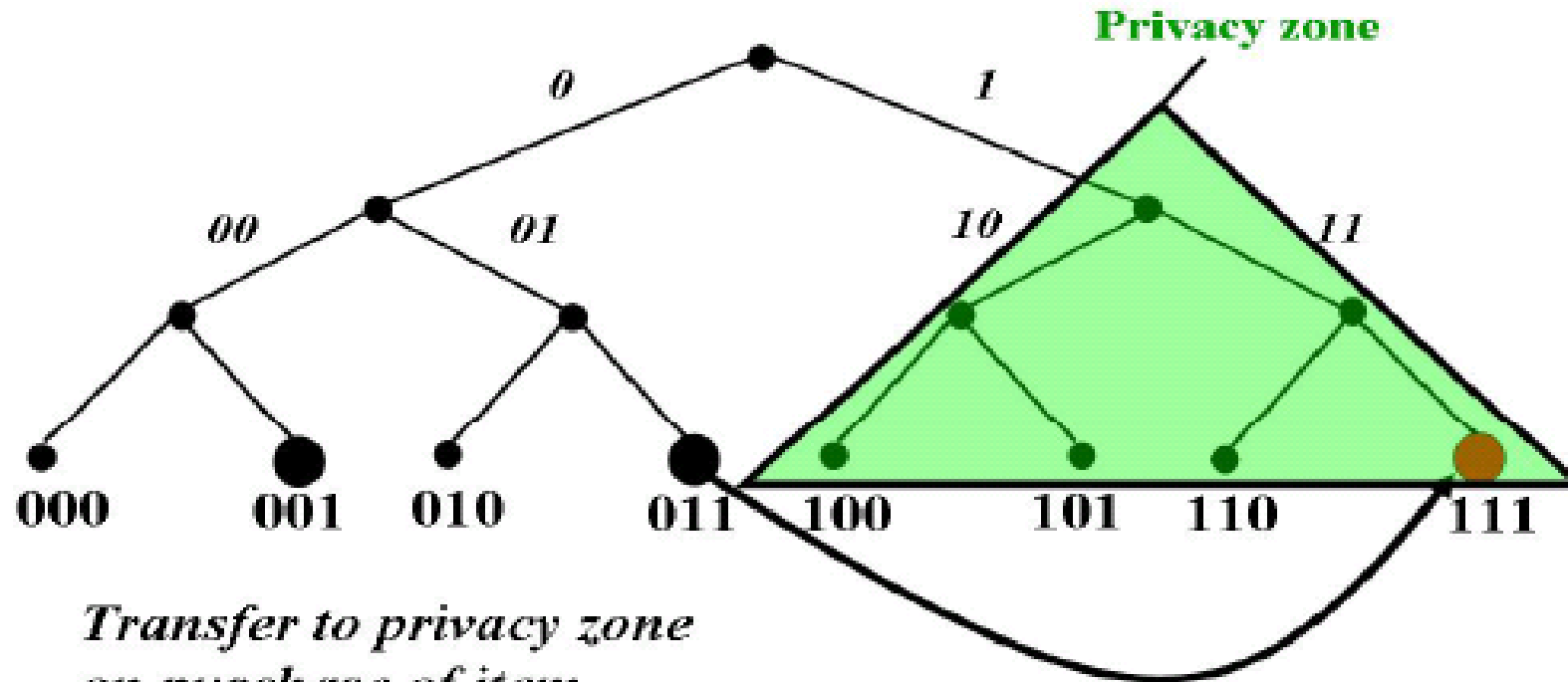
5 – BLOCKING

- “blocker tag” denen etiket sayesinde “privacy zone”daki etiketlerin okunması engellenir
- Bu engelleme işlemi “singulation”dan, yani birden fazla etiketin bir okuyucu tarafından okunması tekniğinden yararlanılarak gerçekleştirilir
- “singulation” tekniklerinden en bilineni “tree walking”dir



5 – BLOCKING

Blocking with tree-walking



*Transfer to privacy zone
on purchase of item*



5 – BLOCKING

- Bir okuyucu bir etiket ortamını sorgularken “blocker tag”in her sorgusuna hem 0 hem de 1 bitini cevap vermesi okuyucunun bütün olasılıkları denemesine neden olur
- Okuyucu “privacy zone”daki etiketleri sorgulamak isterse “blocker tag” bu davranışı gösterir
- Aksi halde okuyucu normal sorgulamasına devam edebilir



5 – BLOCKING

- JRS ayrıca “privacy zone”a girmeden önce okuyucuları uyaran nazik “blocker tag”leri önermiştir
- Sınırlamalar:
 - İyi yerleştirilmiş “blocker tag”ler dahi istenen performansı tam anlamıyla vermeyebilir
 - “blocker tag” sinyallerini filtreleyen okuyucular geliştirilebilir



5 – BLOCKING

Blocking tekniđini kullanan iki alt teknik:

- Soft blocking:

Juels ve Brainard'ın önerisine gre “singulation” tekniđinden yararlanılarak okuyucular engellenmez, “blocker tag” okuyuculara “privacy zone”daki etiketlerin okunmaması gerektiđini syler

- Trusted computing:

Molnar, Soppera ve Wagner okuyucuların tařıdıkları “trusted platform module”ler sayesinde kendilerini izlenen politikaya uyduklarına dair tasdikledikleri bir sistem nermiřlerdir



6 – LEGISLATION

- The US Federal Trade Commission RFID'nin tüketici üzerine etkisini konu edinen daha çok mahremiyet odaklı bir rapor yayınladı
- EPC Global çalışanlarına tüketicilerin RFID etiketlerini kullanabilmesi ve imha edebilmesi yönünde eğitilmesini belirten rehberler dağıttı
- Garfinkel ve Floerkemeier tüketicileri RFID varlığı ve amaçları konusunda bilgilendiren çalışmalar yaptı



B - AUTHENTICATION (ASILLAMA)

- RFID etiketlerinin sahteciliđi, üzerinde bulunduđu ürünün sahteciliđine yol açabilir
- EPC Class-1 Gen-2 tipli etiketler sahteciliđe karşı korumaya sahip değiller
- EPC etiketlerinde bulunan kill PIN normalde okuyucunun kendini etikete asillamasına yarararken, Juels bunun etiketin okuyucuya asillanması için kullanılabileceđini önermiştir



B - AUTHENTICATION (ASILLAMA)

- Etiketler üzerlerinde sahteciliğe karşı geliştirilmiş algoritmalar taşımaları da fiziksel özellikleri bu işlevi gerçekleştirir
- “Physical one-way function” (POWF), madde üzerinde yansıma yapan küçük plastik nesnelere dir
- Bu özelliğe sahip bir maddenin lazerle taranması sonucu oluşan desen o maddeye özgüdür ve bu bilgi bit dizilerine çevrilerek o madde için bir kimlik olarak kullanılabilir



B - AUTHENTICATION (ASİLLAMA)

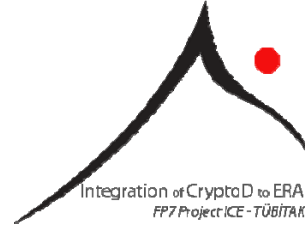
- POWF sahteciliği önleyici iki temel özelliğe sahiptir:
 - Maddeyi fiziksel olarak kurcalamak POWF'un sahip olduğu bilgiyi yok eder veya bozar
 - İstenen bilgiyi verebilecek POWF'a sahip maddeyi oluşturmak neredeyse imkansızdır
- RFID etiketleri POWF bilgilerini içererek unique kimlik sahibi olurlar ve klonlanmaya karşı da bir direnç oluşturmuş olurlar



C – THE PROBLEM OF PIN DISTRIBUTION (PIN DAĞITIM PROBLEMİ)

- Hem mahremiyetin sağlanması için hem de asıllama yapabilmek için PIN'lere ihtiyaç vardır
- EPC Class-1 Gen-2 etiketlerinde kill fonksiyonu için ve yine EPC etiketlerinde yazma erişimi için PIN'e ihtiyaç vardır
- Molnar, Wagner ve Soppera “tree-based” PIN dağıtımını önermişler





TEŞEKKÜRLER

