Üniversite Sanayi İşbirliği Başarılı Uygulamalar Çalıştayı

ODTÜ-UME Tarafından ASELSAN A.Ş. İçin Gerçekleştirilen Projeler

Ar. Gör. Çağdaş Çalık

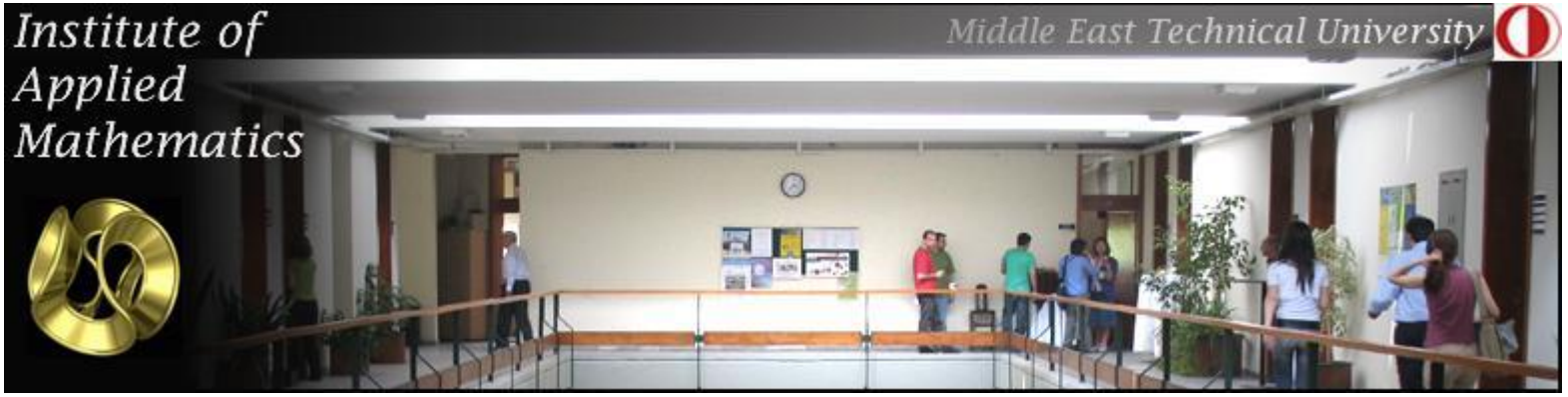
Uygulamalı Matematik Enstitüsü

ODTÜ

İçerik

- ODTÜ – UME Tanıtımı
- Projeler
  - Blok Tipi Algoritmaların İstatistiksel ve Yapısal Test Yazılımlarının Geliştirilmesi
  - Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi
  - Eşleme-Tabanlı Kripto Sistemleri Araştırma Geliştirme Projesi
- Değerlendirmeler

ODTÜ - UME



- 21 Haziran 2002'de kuruldu. 2002-2003 sonbahar döneminde eğitim faaliyetine başladı.
- Kriptografi, Bilimsel Hesaplama, Finansal Matematik, Aktüerya Bilimleri programlarında lisansüstü eğitim.
- Matematik temelli disiplinlerarası işbirliğini geliştirmek, eğitim ve araştırma faaliyetleri yürütmek.
- http://www.iam.metu.edu.tr

Kriptoloji Laboratuvarı

- Devlet Planlama Teşkilatı desteğiyle 2006 yılında inşa edildi.
- Toplam 34 araştırmacının çalışabileceği laboratuvarlar, kütüphane, seminer odası, toplantı odaları ve idari ofisler.

Projeler

Proje Adı: Blok Tipi Algoritmaların İstatistiksel ve Yapısal Test Yazılımlarının Geliştirilmesi
Yürütücüsü: Ali Doğanaksoy
Süresi: 1.12.2006-30.11.2007
Bütçesi: 100.000 YTL

Projenin Adı: Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi
Yürütücüsü: Ersan Akyıldız, Rüyal Ergül
Süresi: 1.10.2006-30.3.2008
Bütçesi: 200.000 TL

Proje Adı: Eşleme-Tabanlı Kripto Sistemleri Araştırma Geliştirme Projesi
Yürütücüsü: Ersan Akyıldız
Süresi: 01.12.2008-30.06.2009
Bütçesi: 30.000 USD

Blok Tipi Algoritmaların İstatistiksel ve Yapısal Test Yazılımlarının Geliştirilmesi

- Projenin Oluşum Öyküsü
  - ASELSAN'da geliştirilen kripto cihazları için özgün olarak tasarlanan kripto algoritmaları güvenlik testleri için sertifikasyon laboratuarında test ve analiz edilmekte ve buna göre ancak gizlilik onayı aldıktan sonra kullanılabilmektedir.
  - Algoritma geliştirme aşamasında uygulanabilecek yapısal ve istatistik test altyapısının ASELSAN'da oluşturulması ile algoritma test ve analiz süreçlerinin kısalması, algoritma tasarım süreçlerinin iyileştirilmesi hedeflenmiştir.
  - Bu amaçla özellikle yoğun matematiksel teorik altyapı ve aynı zamanda kriptoloji konusunda temel ve güncel etkin bilgi birikimi gerektiren bu konuda üniversite işbirliği arayışına gidilmiş, bu konuda Türkiye'deki yetkin tek enstitü olan ODTÜ-UME ile işbirliğine gidilmesine karar verilmiştir.

Blok Tipi Algoritmaların İstatistiksel ve Yapısal Test Yazılımlarının Geliştirilmesi

- Blok Şifreler
  - Simetrik Anahtarlı Kriptosistemler
  - İletilen ya da depolanan verinin gizliliğinin/bütünlüğünün sağlanması

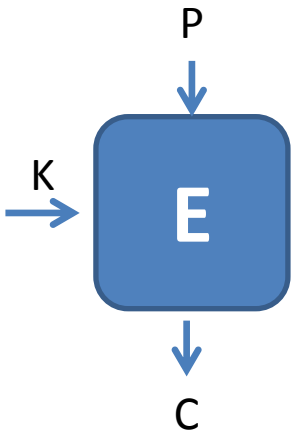
Şifreleme **Deşifreleme**

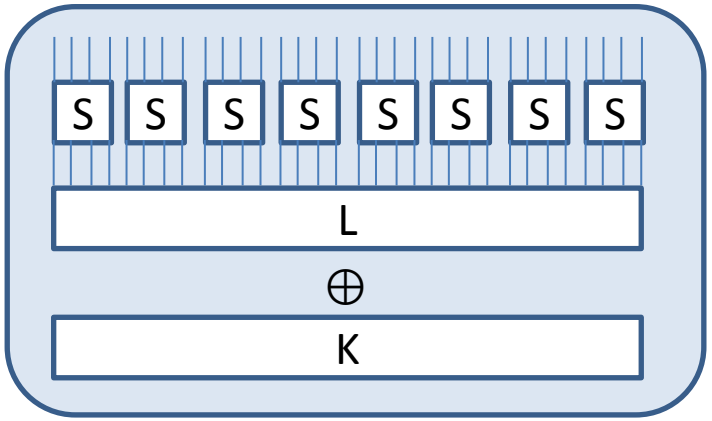
Blok Tipi Algoritmaların İstatistiksel ve Yapısal Test Yazılımlarının Geliştirilmesi

- Projenin Amacı
  - Tanımlanan bir blok şifrenin istatistiksel ve yapısal zaafiyetlerinin olup olmadığının belirlenmesi
  - Temel kriptanaliz yöntemlerine karşı dayanıklılığın ölçülmesi

Blok Tipi Algoritmaların İstatistiksel ve Yapısal Test Yazılımlarının Geliştirilmesi

- Yöntem
  - Kara Kutu (Black-box) test
    - Blok şifreden test verisi üretmek
    - Literatürde bulunan ve kendi tanımladığımız istatistiksel testleri uygulamak
    - Girdi ve çıktı bitleri arasındaki ilinti miktarını ölçmek
  - Açık Kutu (White-box) test
    - Blok şifrelerin tanımlanabildiği bir dil oluşturmak
    - Blok şifrenin bileşenlerinin analiz edilmesi
    - Blok şifrenin diferansiyel ve doğrusal kriptanaliz yöntemlerine karşı dayanıklılığının hesaplanması





Blok Tipi Algoritmaların İstatistiksel ve Yapısal Test Yazılımlarının Geliştirilmesi

- Projenin ASELSAN'a katkıları
  - Geliştirilen proje ile ASELSAN bünyesinde mevcut algoritma test ve analiz altyapısına yeni yetenek kazandırılmıştır.
  - 2007 yılından itibaren bahse konu yetenek ASELSAN süreçlerinde etkin olarak kullanılmaktadır.
  - Proje, ASELSAN süreçlerinde zaman ve işçilik açısından ekonomik katkı sağlamıştır.
  - ASELSAN tarafından geliştirilen tüm kriptografik ürünlerde bu yeteneğin kullanılması ile milli projelere ulusal katkı sağlanmıştır.

Blok Tipi Algoritmaların İstatistiksel ve Yapısal Test Yazılımlarının Geliştirilmesi

- ÜSİ'deki Başarı Faktörleri
  - Proje ile geliştirilen yetenek algoritma tasarlama ve geliştirme süreçlerinde maliyet etkin olarak kullanılmaktadır.
  - Bu yetenek kullanılarak ASELSAN tarafından geliştirilen algoritmaların, Ulusal ve Uluslar arası Sertifikasyon Merkezlerinde gerçekleştirilen test süreçlerinden başarı ile geçmekte olduğu bildirilmiştir.

Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi

- Projenin Oluşum Öyküsü
  - Açık anahtarlı kriptografide teknolojik gelişmelere bağlı olarak artan güvenlik gereksinimlerini RSA bazlı algoritmalara kıyasla daha kısa anahtar boylarında ve dolayısıyla daha yüksek performansla karşılayan eliptik eğrilerin kullanımı giderek yaygınlaşmaktadır. Aselsan A.Ş.'nin geliştirdiği kriptografik ürünlerde de eliptik eğri teknolojisine geçilmesi gerekliliği değerlendirilmiştir.
  - Bu amaçla özellikle yoğun matematiksel teorik altyapı ve aynı zamanda kriptoloji konusunda temel ve güncel etkin bilgi birikimi gerektiren bu konuda üniversite işbirliği arayışına gidilmiş, bu konuda Türkiye'deki yetkin tek enstitü olan ODTÜ-UME ile işbirliğine gidilmesine karar verilmiştir.

Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi

- Amaç
  - Eliptik Eğri Tabanlı Kriptografi kütüphanesi geliştirilmesi
    - Eliptik Eğri Diffie-Hellman Anahtar Paylaşımı
    - Eliptik Eğri Sayısal İmza Algoritması

Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi

- Eliptik Eğri Kriptografisi
  - Açık Anahtarlı Kriptosistemler
  - 1985 yılında Miller ve Koblitz tarafından önerildi.
  - RSA'nın alternatifi
    - Daha hızlı
    - Daha az hafıza
  - Güvenliği Eliptik Eğri Ayrık Logaritma probleminin zorluğuna dayanır.

Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi

- Güvenlik seviyeleri karşılaştırması

Tablo 1. Güvenlik Seviyelerine Uygun Olarak Kullanılan Kriptografik Algoritmalar, Anahtarların bit Uzunlukları ve Son Geçerlilik Tarihleri

Güvenlik Seviyeleri / *Algoritmalar*	Sınıflandırılmamış	Gizli(Kısa Süreli Koruma)	Gizli(Orta Vadeli Koruma)	Gizli(Uzun Süreli Koruma)	Çok Gizli(Askeri Gizlilik Düzeyi)
Simetrik					
2DES	80				
3DES		112			
AES			128	192	256
Asimetrik					
DSA[1]	1024 -160	2048 - 224	3072 - 256	7680 - 384	15360 - 512
RSA	1024	2048	3072	7680	15360
ECDSA	160	224	256	384	512
EC	160	224	256	384	512
Diffie-Hellman	1024	2048	3072	7680	15360
Özet Fonksiyonları					
RIPEMD	160				
SHA		224	256	384	512
Son Geçerlilik Tarihi*	2010	2020	2030	2050	**

[1] İlk değer grubun boyutunu, ikinci değer anahtar uzunluğunu göstermektedir.
* Günümüz koşullarına uygun olarak yaklaşık değerler verilmiştir.
** Kuantum bilgisayarlara karşı iyi koruma sağlamaktadır.

Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi

- RSA – Eliptik Eğri Performans Karşılaştırması

Tablo 4 E-imza Algoritmalarının Performansları

Algoritma	imza sayısı /dakika	Algoritma	imza sayısı /dakika
RSA 1024 bit imzalama		**ECDSA 192 bit imzalama**	
RSA 1024 bit imza doğrulama		**ECDSA 192 bit imza doğrulama**	
RSA 2048 bit imzalama	2940	**ECDSA 224 bit imzalama**	105840
RSA 2048 bit imza doğrulama	26880	**ECDSA 224 bit imza doğrulama**	47520
RSA 3072 bit imzalama	480	**ECDSA 256 bit imzalama**	54000
RSA 3072 bit imza doğrulama	11280	**ECDSA 256 bit imza doğrulama**	22800
RSA 7680 bit imzalama	60	**ECDSA 384 bit imzalama**	30960
RSA 7680 bit imza doğrulama	2160	**ECDSA 384 bit imza doğrulama**	11040
RSA 15360 bit imzalama	60	**ECDSA 521 bit imzalama**	14400
RSA 15360 bit imza doğrulama	480	**ECDSA 521 bit imza doğrulama**	5280

Tablo 4'deki veriler Pentium IV 3.0 GHz işlemcili bir bilgisayarda elde edilmiştir.

Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi

- Projenin ASELSAN'a Katkıları
  - Geliştirilen proje ile ASELSAN eliptik eğri teknolojisi kullanılarak sayısal imzalama ve anahtar değişim protokolleri gerçekleme yeteneği kazanmıştır.
  - Söz konusu protokoller ASELSAN tarafından geliştirilen kriptografik ürünlerde kullanılmıştır.
  - Böylece hem ASELSAN'a ekonomik katkı hem de kullanıldığı milli projelere ulusal katkı sağlamıştır.

Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi

- ÜSİ'deki Başarı Faktörleri
  - Proje ile geliştirilen eliptik eğri tabanlı kriptografik protokoller kriptografik ürünlerde maliyet etkin olarak kullanılmaktadır.

Eşleme-Tabanlı Kripto Sistemleri Araştırma Geliştirme Projesi

- Projenin Oluşum Öyküsü
  - Kriptografideki gelişmeler doğrultusunda özellikle bant genişliğinin kısıtlı olduğu uygulamalarda eşleme-tabanlı (pairing-based) kripto sistemleri tercih edilmeye başlanmıştır.
  - Eliptik eğrilere dayalı eşlemeler üzerine geliştirilen Kısa İmzalama (Short Signatures), Kimlik Tabanlı İmzalama (Identity-Based Signatures), Üç-Taraflı (Tripartite) Diffie-Hellman Anahtar Değişimi ve Kimlik Tabanlı Şifreleme metodu (Identity Based Encryption) gibi protokollerin kullanılması hedeflenmiştir.
  - Bu amaçla özellikle yoğun matematiksel teorik altyapı ve aynı zamanda kriptoloji konusunda temel ve güncel etkin bilgi birikimi gerektiren bu konuda üniversite işbirliği arayışına gidilmiş, bu konuda Türkiye'deki yetkin tek enstitü olan ODTÜ-UME ile işbirliğine gidilmesine karar verilmiştir.

Eşleme-Tabanlı Kripto Sistemleri Araştırma Geliştirme Projesi

- Amaç
  - Eşleme Tabanlı Kriptografi kütüphanesi oluşturmak
    - Tek döngüde 3 taraflı anahtar paylaşımı
    - Kısa imzalama protokolleri
    - Kimlik tabanlı imzalama
    - Sistemin verimli çalışmasına olanak veren matematiksel cisimlerin seçilmesi

Eşleme-Tabanlı Kripto Sistemleri Araştırma Geliştirme Projesi

Üçlü Anahtar Paylaşımı

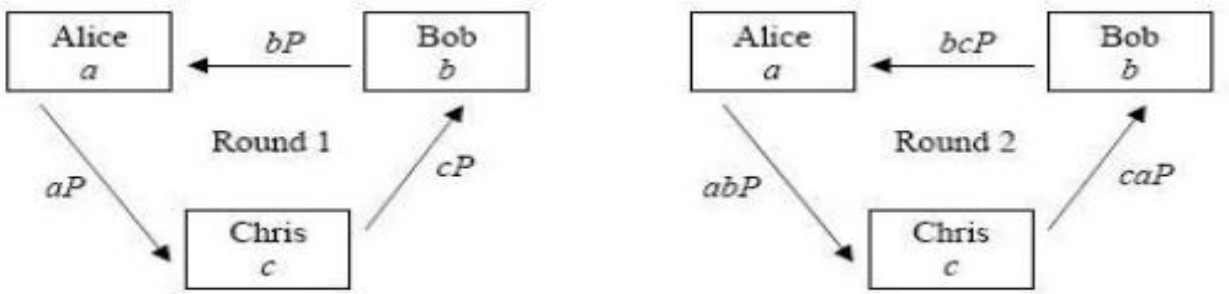


Figure: Iki Dongude Uclu Anahtar Paylasimi

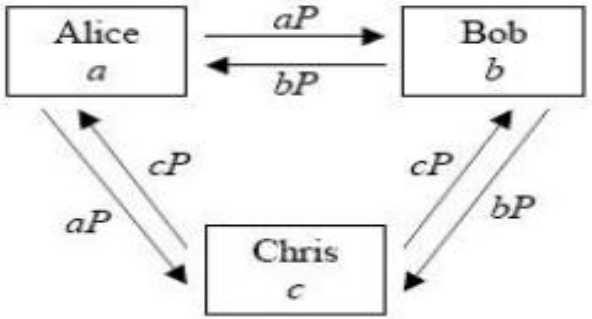


Figure: Tek Dongude Uclu Anahtar Paylasimi

Eşleme-Tabanlı Kripto Sistemleri Araştırma Geliştirme Projesi

- Projenin ASELSAN'a katkıları
  - Geliştirilen proje ile ASELSAN bant genişliğinin ve sistem kaynaklarının az olduğu mobil uygulamalarda eşleme tabanlı protokolleri gerçekleme yeteneği kazanmıştır.
  - Söz konusu protokoller ASELSAN tarafından geliştirilen mobil kriptografik ürünlerde maliyet etkin olarak kullanılmıştır.

Eşleme-Tabanlı Kripto Sistemleri Araştırma Geliştirme Projesi

- ÜSİ'deki Başarı Faktörleri
  - Proje ile geliştirilen eşleme tabanlı protokoller mobil uygulamalara sahip projelerde başarı ile kullanılmaktadır.

Değerlendirme

- ÜSİ Sürecinde Karşılaşılan Zorluklar
  - Bu projelerde, ÜSİ kapsamında ODTÜ-UME ile ASELSAN birlikte hazırlanan ve karşılıklı olarak imzalanan sözleşmelerle ve özellikle sözleşme ekleri olan
    - İş tanımı
    - Teslimat planı
    - Sözleşme doküman listesi
    - Ödeme planı
    - Gizlilik antlaşması

  dokümanları ile ÜSİ süreçleri sorunsuz ve planlandığı gibi gerçekleşmiştir.

Değerlendirme

- Kazanımlar
  - Proje konularında bilgi birikimi olgunlaşmış, nitelikli araştırmacılar yetişmiştir.
  - Belgelendirilen çalışmalar, yeni araştırmacılar için faydalı bir kaynak oluşturmaktadır.
  - Proje çıktılarının bazıları araştırmacıların akademik çalışmalarında da kullanılabilmektedir.
- Öneriler
  - Projelerde tek taraflı fayda sağlanması yerine karşılıklı çıkar elde edilmesine çalışılmalıdır.
  - Proje çıktılarının kullanımı konusunda geribildirim verilerek iyileştirme / ince ayarlama yapmak suretiyle daha verimli bir kullanım sağlanabilir.
  - Proje süresince edinilen tecrübeler, ortaya çıkan bulgular makale / bildiri şeklinde yayınlanabilir.

Teşekkürler.