TÜBİTAK-ARDEB

Bilgi Güvenliği Çağrı Programı

"1003-BIT-BGUV-2017-1 Kriptoloji"

Çağrı Metni

1. Genel Çerçeve

Kriptoloji çağımızın en önemli araştırma alanlarından birisidir. Gerek kuramsal çalışmalar, gerek uygulamalarının yaygınlığı, gerekse pratikte kullanılan yöntemlerin standartlaştırılması açısından çok büyük öneme sahiptir. Kriptoloji konusunu diğer güvenlik yöntemlerinden ayıran en büyük etken "kanıtlanabilir güvenlik" sunmasıdır. Kriptolojik çalışmalarda bir sistemin güvenliği matematiksel veya hesaplamasal problemlere dayandırılarak kanıtlanır. Kriptografik algoritmaların geliştirilmesindeki karşıt kısıt da performanstır. Güvenlik garantileri ile birlikte sağlanması gereken kısıtlar, yüksek hızlı, düşük bellek izi, çeşitli yazılım/donanım mimarisi kısıtlarında çalışabilmedir. Çağrı kapsamında önerilen Ar-Ge çalışmalarının uygulanabilir olması da çağrı açısından önemlidir. Bu da akademi-sanayi işbirliğini ön plana çıkarmaktadır.

Kriptoloji alanında güçlü ve yenilikçi AR-GE faaliyetlerini teşvik eden bu çağrı ile donanımsal/yazılımsal/algoritmik çalışmaların desteklenmesi, projelendirilmesi ve hayata geçirilmesi amaçlanmaktadır.

2. Amaç ve Hedefler

Bu çağrı kapsamında aşağıda yer alan konu başlıklarında yenilikçi ve özgün projelerin desteklenmesi hedeflenmektedir.

a) Kriptoloji uygulamaları geliştirilmesi

- Güvenliği ve gizliliği koruyucu iletişim (metin, ses, görüntü) uygulamaları geliştirilmesi (mobil, masaüstü, özel donanım).
- Dış kaynak kullanımında (örneğin bulut) hem veri akışının, hem veri depolamasının, hem de veri işlemesi aşamasının gizliliğini ve güvenliğini sağlayan yeni kriptolojik çözümler ve bu çözümleri gerçekleyen sistemler geliştirilmesi.
- Gizliliği koruyan veri işleme sistemlerinin hem sistemsel hem kriptolojik olarak yenilikçi çözümlerle sağlanması ve pratik çalışmasının gösterilmesi.
- Disk şifreleme, dosya ve klasör şifreleme, kimlik denetimi gibi uygulamalı konularda kriptolojik çözümler kullanan yerel sistemler geliştirilmesi.
- Uygulama alanı olan, şimdi veya yakın gelecekte uygulamaya geçmesi planlanan konularda kuramsal kriptolojik çalışmalar yapılması.
- Görevdeş (peer-to-peer) sistemlere yönelik kriptolojik yaklaşımlar geliştirilmesi.
- İki veya daha çok kişinin yer aldığı protokollerde (hesaplama, takas, bilgi dağıtımı, vs.) güvenliği ve gizliliği koruyan yeni kriptolojik çözümler geliştirilmesi ve bunların gerçeklenmesi.
- Değişik veri tiplerine yönelik en iyileştirilmiş çözümlerin geliştirilmesi. Örneğin, metin, ses, görüntü, çok gizli belge, değişmeyen veri, sürekli güncellenen veri, akışkan veri vs. için en iyi yöntemlerin seçilmesi, yeni kriptolojik çözümlerin geliştirilmesi ve bu seçimi otomatik yapan bir sistem geliştirilmesi.
- Yaygın şifreleme algoritmalarının kısıtlı kaynaklar (düşük güç, işlemci, hafıza)

altında çalışmak üzere etkin gerçeklenmesi.
- Kriptolu IP tabanlı haberleşme uygulamalarının geliştirilmesi.
- Gizliliği koruyucu veri yönetimi uygulamalarının geliştirilmesi.
- Şifreli veriler üzerinde arama yapabilmesine izin veren kriptografik yaklaşımlar, gizliliği ve formatı koruyan uygulanabilir şifreleme teknikleri geliştirilmesi.

b) Kuantum kriptoloji yaklaşımlarının geliştirilmesi

- Kuantum anahtar dağıtımı çözümlerinin gerçeklenmesi ve denemelerinin başarılı olduğunun gösterilmesi.
- Kuantum bilgisayarlar ve kuantum iletişim kanallarıyla çalışan yenilikçi kuantum kriptografi çözümleri (kuantum anahtar dağıtımı harici).
- Post kuantum kripto algoritma ve sistemlerinin geliştirilmesi.

c) Kriptanaliz yapılması

- Güncel, özellikle yakın zamanda dünya çapındaki yarışmalardaki ve yayınlardaki, kriptolojik çalışmaların kriptanaliz yöntemleriyle kırılması ve eğer pratik bir saldırı bulunursa bunu gerçekleyen bir araç geliştirilmesi.
- Yaygın kullanılan kriptoloji yöntemleri ve araçlarına yönelik kriptanaliz çalışmaları yapılması ve bulunan açıklara kriptolojik çözümler geliştirilmesi.

d) Donanımsal kriptografik çözümler geliştirilmesi

- Kriptografik algoritmaların donanımsal platformlar üzerinde verimli ve güvenli gerçeklemeleri.
- Gömülü sistemler üzerinde hızlı, verimli ve güvenli kriptografik algoritmalar ve yazılımlarının gerçeklenmesi.
- Kripto çiplerinin/cihazlarının yazılımları.

3. İlgili Destek Programı

Bu çağrı konusu kapsamında önerilecek projelere “1003-Öncelikli Alanlar Ar-Ge Projeleri Destekleme Programı” kapsamında destek verilecektir.

4. Çağrıya Özel Hususlar

- Önerilecek projeler küçük, orta veya büyük ölçekli projeler olarak hazırlanabilir.
- Bu çağrı kapsamında altyapı oluşturmaya yönelik olan projeler desteklenmez ve proje bütçe kalemleri arasında dengeli bir dağılım olması beklenir.
- Söz konusu çağrı programının ARDEB bünyesinde gerçekleştiği göz önünde bulundurularak çalışmaların bilimsel araştırma niteliğinin de bulunması beklenmektedir. Entegrasyon/montaj içeren pilot uygulama projeleri destek kapsamı dışındadır.
- Farklı disiplinlerden araştırmacıların proje ekibinde görev alması ve konunun disiplinler arası bir yaklaşımla ele alınması önerilmektedir.
- Orta ve büyük ölçekli projelerin farklı kurum/kuruluşlarda yürütülen ve birden fazla kurumun yer aldığı alt projelerden oluşması (bir proje en fazla 1 ana ve 3 alt projeden oluşabilir) ve üniversite ile özel sektörün katılımı önerilmektedir.
- Ortaklı projelerde özel sektörün projeye ayni/nakdi destek sağlamış olması gerekmektedir. İlgili destek mektubu 2. Aşama proje önerisine eklenmelidir.

- Bu çağrı programına önerilecek projelere, yeni kurulan üniversitelerden (2006 yılından itibaren kurulmuş üniversiteler) proje yürütücüsü ve/veya araştırmacıların katılımının sağlanması teşvik edilmektedir (*).

(*) Bilimsel değerlendirme sırasında aynı/yaklaşık puan alan proje önerilerinden belirtilen koşulu sağlayanlara bütçe imkanları da gözetilerek öncelik sağlanacaktır.

5. Çağrı Takvimi

	Çevrimiçi Başvuru Sistemi Kapanış Tarihi	Elektronik Başvuru Çıktısının Gönderilmesi İçin Son Tarih (*)
Birinci Aşama	17.02.2017 17:30	24.02.2017 17:30
İkinci Aşama	26.05.2017 17:30	09.06.2017 17:30

(*) Elektronik başvuru çıktısının ıslak imzalı nüshasının belirtilen tarih ve saate kadar Kurumumuza ulaştırılması gerekmektedir.

6. Ek Belgelere Referanslar

- 1003 Destek Programı Web Sayfası
- 1003 Destek Programı Bilgi Notu
- 1003 Öncelikli Alanlar Ar-Ge Projeleri Destekleme Programı Usul ve Esasları
- Ulusal Bilim, Teknoloji ve Yenilik Stratejisi (UBTYS) 2011-2016
- 1003 Proje Önerisi Değerlendirme Formu
- Yasal/Özel İzin Belgesi Bilgi Notu
- Etik Kurul Onay Belgesi Bilgi Notu

7. İrtibat Bilgileri

Altuğ ÇİL

Tel	0312 298 12 27
e-posta	altug.cil@tubitak.gov.tr

Elektrik, Elektronik ve Enformatik Araştırma Destek Grubu (EEEAG)