RFID Etiketlerinde Hafifsıklet Kriptografi ve Kademeli Güvenlik

Ilgın Şafak[1], Mustafa Başak[2]

[1] Progress Ar-Ge Merkezi, Provus Bilişim Hizmetleri A.Ş., İstanbul
[2] SIM-ANT Bilgi İşlem Ltd. Şti, İstanbul
ilgin.safak@provus.com.tr, mustafabasak@sim-ant.com
(Bu çalışma TÜBİTAK TEYDEB 3130823 no.lu proje tarafından desteklenmiştir.)

Özet: Günümüzde güvenlik, sağlık, perakende sektörü, vb. birçok alanda kişi veya cisimlerin tanınması ve takip edilmesinde pasif (güç kaynağı olmayan) radyo frekans kimlik (radio frequency identification, RFID) elektronik etiketlerinin kullanımı yaygınlaşmaktadır. Ancak bunun beraberinde tüketici mahremiyeti, endüstriyel sabotaj, etiket kopyalama, vb. güvenlik ve gizlilik sorunları ile karşılaşılmaktadır. Bu tür sorunların önlenmesinde RFID etiketlerinde kriptografik yöntemlerin kullanılması önemlidir. Ancak RFID etiketlerindeki donanım, güç tüketimi ve maliyet ile ilgili kısıtlamalar nedeniyle güvenlik, maliyet ve başarım arasında ödünleşim bulunmaktadır. Bu çalışmada, pasif RFID etiketleri için hafifsıklet kriptografik ile kademeli güvenlik koruması sağlayan yöntemler incelenmiştir.

Anahtar Sözcükler: RFID, Elektronik Etiket, Hafifsıklet Kriptografi, Bilgi Güvenliği, Kademeli Güvenlik.

Lightweight Cryptography for RFID Tags and Multi-Stage Security

Abstract: Passive radio frequency identification (RFID) tags are used in detecting and tracking people and items by sectors such as security, health, and supply chains. However, this raises certain security and privacy concerns such as consumer privacy, industrial sabotage and tag cloning, where cryptography is essential in alleviating such safety concerns. On the other hand, due to hardware, power consumption and cost limitations in RFID tags, there is a trade-off between safety, cost and performance. In this paper, lightweight cryptography that provides multi-stage safety measures in passive RFID tags is examined.

Keywords: RFID, Electronic Tag, Lightweight Cryptography, Information Security, Multi-Stage Security.

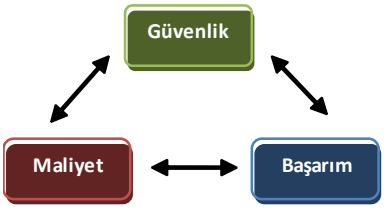
1. Giriş

RFID teknolojisi kişi veya cisimlerin telsiz olarak tanınması ve takip edilebilmesi açısından cazip bir çözüm sunduğundan günümüzde birçok sektörde yaygın olarak kullanılmaktadır. RFID teknolojisi sayesinde örneğin, hapishane mahkûmları takip edilebilmekte, hızlı ve otomatik ödeme yapılabilmekte, tedarik zincirlerinde stok otomatik olarak izlenebilmekte, mağazalarda hırsızlıklar önlenebilmekte ve tüketiciler ürün hakkında bilgi edinebilmektedirler [1]-[2].

Ancak, RFID teknolojisinin yaygınlaşması ile birlikte güvenlik ve gizlilik sorunları da önem kazanmıştır. Tüketicilerin satın aldıkları ürünlerden takip edilebilmeleri ciddi bir gizlilik sorunu teşkil etmektedir. Başka önemli bir gü-

venlik endişesi, RFID etiketlerin kopyalanarak sahte ürünlerde veya izinsiz geçiş vb. durumlarda kullanılmalarıdır. Ayrıca RFID etiketlerinin etkisiz hale getirilmesi veya içeriğinin değiştirilmesi ile hırsızlık veya endüstriyel sabotaj yapılması güvenlik açıkları arasındadır [1]-[2].

RFID etiketlerinin güvenliğini artırmak için çeşitli önlemler alınabilir. RFID etiketinin özel bir şekilde geliştirilerek yeniden kullanılması ve kopyalanması fiziksel olarak engellenebilir [3]. Örneğin, Türkiye'de köprü ve otoyollarda otomatik geçiş ve ödemede kullanılan hızlı geçiş sistemi (HGS) RFID etiketleri yalnızca bir kez yapıştırılır olma özelliğine sahiptirler. Araç camına yapıştırılmış olan HGS etiketi çıkartılmak istendiğinde deforme olarak geçersiz hale gelmektedir [4].



Şekil 1. Maliyet, güvenlik ve başarım arasındaki ödünleşim

Fiziksel önlemler etiket kopyalama, etiket etkisizleştirme, gizli dinleme [5] vb. saldırılarına karşı tek başına tedbir sağlamamaktadır. Bu nedenlerle, fiziksel tedbirlerin yanı sıra donanımsal önlemlerinin (kriptografik bileşen, güvenli veri saklanma, güvenlik sensörleri) de alınması gerekmektedir [3]. Donanımsal güvenlik önlemlerinin arasında kriptografi özellikle büyük önem arz etmektedir, ancak RFID etiketlerin güvenliğini artırmak donanımsal karmaşıklığı, güç tüketimini ve maliyeti de artırmaktadır [6]-[9]. Bu durum özellikle güç tüketimi kısıtlaması altında çalışmak zorunda olan RFID etiketleri için hiç arzu edilmez. Dolayısıyla güvenlik, maliyet ve başarım arasında bir ödünleşim (bkz. Şekil 1) sağlanması zorunluluğu ortaya çıkar [8]. Bu çalışmada düşük maliyet ve düşük işlem gücüne sahip RFID etiketlerinde olabildiğince yüksek güvenlik sağlayan kriptografik yöntemler incelenmiştir.

2. RFID Sistemleri

RFID teknolojisi RF dalgaları aracılığı ile cisimlerin kimliklerinin belirlenmesi ve izlenmesi için kullanılır [1]-[2]. Bir RFID sistemi, okuyucu, etiket ve sunucu olmak üzere üç ana bileşenden oluşmaktadır (bkz. Şekil 2). Sunucu, okuyucudan gelen bilgileri işleyen birimdir. Okuyucu, etiketi algılayan, etiketin içerisindeki bilgiyi okuyan ve kendi güç kaynağı olan bileşendir. RFID etiket okuyucusu ve RFID etiketi, birbirleri ile yakın alan iletişimi veri alış-verişinde bulunurlar. RFID etiketi ise düşük güç tüketen ve okuyucunun istediği bilgileri göndermekle görevli birimdir. Tükettiği sınırlı gücü kendisi üretebildiği gibi, okuyucudan gelen yakın alan RF dalgalarından ya da başka yöntem ile hasat edebilir [1]-[2].

Şekil 2. Pasif UHF RFID Sistemi

RFID sistemleri, düşük frekans (low frequency, LF) 125–134 kHz, yüksek frekans (high frequency, HF) 13.56 MHz, ultra yüksek frekans (ultra high frequency, UHF) 860–960 MHz, 2.45 GHz ve süper yüksek frekans (super high frequency, SHF) 5.8 GHz frekans olmak üzere dört farklı frekans bandında çalışabilmektedirler. Okuyucu ve etiket arasındaki uzaklık birbirlerinin yakın alanlarında bulunacağı şekilde seçilir ve aralarındaki bilgi alış-verişi döngü antenler arasındaki manyetik etkileşim aracılığı ile sağlanır [1]-[2].

RFID etiketi, yonga, döngü (loop) anten ve kaplamadan oluşan minyatür bir radyo modülüdür. Anten, yongaya veri ve/veya enerji transferi yapan bileşen; yonga, etiket ile ilgili bilgileri saklayan ve veri işleme yapan bileşen; kaplama, anten ve yongayı çevresel koşullardan koruyan bileşendir. Güç kaynağı içerme durumuna göre RFID etiketleri aktif, yarı-pasif ve pasif olmak

üzere üç farklı yapıda olabilir. Aktif etiket, kendi güç kaynağını kullanarak belirli aralıklarla kimliğini yayımlar. Yarı-pasif etikette bulunan küçük bir pil, RFID okuyucusuna yaklaştığında devreye girerek yongayı çalışır konuma getirir ancak veri iletiminde okuyucunun RF sinyali kullanılır. Pasif etiketlerde ise pil bulunmadığından yonganın çalışması ve veri iletimi için gerekli olan enerji transferi RFID okuyucusundan yapılır. Okuyucudan pasif etiket yönündeki iletişim, okuyucunun ürettiği zamanla değişen manyetik alanın etiket sargısının üzerinde oluşturduğu gerilim ile sağlanır. Yonga, sargı üzerindeki gerilimi doğru akıma çevirerek aktif hale gelir ve hasat ettiği elektrik enerjisini kullanarak istenilen kimlik vb. bilgileri belirli bir zaman aralığı içerisinde okuyucuya iletir [1]-[2]. Örneğin, HGS altyapısında bulunan RFID etiketi bir pasif etikettir [4]. Düşük birim maliyete sahip, pratik ve dayanıklı olmalarından dolayı pasif RFID etiketlerinin kullanımı yaygınlaşmaktadır. Bu çalışmada pasif RFID etiketlere yönelik güvenlik ve gizlilik sağlayan kriptografik çözümler ele alınacaktır.

3. Pasif RFID Etiketleri için Hafifsiklet Kriptografi

Kriptografik işlemlerinin arasında önemli bir yer teşkil eden doğrulama hizmeti, kimlik (entity) ve mesaj doğrulaması olmak üzere ikiye ayrılmaktadır. RFID etiketinin geçerliliğinin denetlenmesinde kimlik doğrulama yöntemi kullanıldığından, bu çalışmada yalnızca kimlik doğrulama yöntemleri ele alınmıştır. Kimlik doğrulamanın bir yolu, şifreli bir mesajı şifre çözerek özel anahtar bilgisinin olduğunu ispatlamaktır. Kimlik doğrulamanın bir başka yolu da bir sorgunun imzalanmasıdır. İmzaya dayalı kimlik doğrulama yönteminde genelde tekyönlü hash fonksiyonu kullanılmaktadır [5]. RFID etiketleri için kullanılan kimlik doğrulama çözümlerinin bazıları aşağıda özetlenmiştir.

[10]'da, RFID etiketi ve okuyucusu arasında 128-bit Advanced Encryption Standard (AES) algoritması ile sorgu-cevap modeline dayalı güçlü doğrulamanın yapıldığı bir protokol geliştirilmiştir. Geliştirilen AES algoritmalı protokol, RFID etiketleri için hızlı, az güç tüketen ve düşük donanım karmaşıklıklı tek yönlü doğrulama çözümü sunmaktadır [10]. Ancak [10]'daki yöntemin tekrarlama (replay) ve etiket kopyalama saldırılarına karşı açık olduğu gösterilmiştir [11]. [11]'de AES ile karşılıklı doğrulama yapılarak, [10]'daki bazı güvenlik açıkları kapatılmıştır. Ancak [11]'deki yöntemde, etiket ve okuyucu arasındaki senkronizasyon kolayca bozulabilmekte ve ortadaki adam saldırısına karşı savunmasız olması önemli bir güvenlik açığıdır [12]. [12]'de, [11]'deki yöntem üzerinde iyileştirmeler yapılarak güvenlik açıklarının giderildiği, 128-bit AES ile sorgu-cevap yöntemli karşılıklı doğrulamanın yapıldığı bir protokol geliştirilmiştir. Geliştirilen karşılıklı doğrulama protokolü sayesinde RFID etiketi ve sunucu arasında şifreli veri iletimi gerçekleştirilerek etiket izleme, gizli dinleme, vb. güvenlik saldırılarına karşı korunmaktadır. Ayrıca etiketin içerisinde ve sunucuda saklanan özel anahtarın her doğrulama oturumunda güncellenmesi ile tekrarlama saldırısı önlenmektedir.

Simetrik anahtarlı şifreleme ile gizlilik ve veri güvenliği sağlanabilmekte, ancak özel anahtarların güvenli bir şekilde paylaşılması ve yönetilmesi konusunda ciddi sıkıntılar bulunmaktadır [6]-[9]. Bu sorun, asimetrik anahtarlı şifreleme [5] ile hafifletilebilir, ayrıca RFID etiketlerinin merkezi bir şekilde açık anahtar altyapısı (public key infrastructure, PKI) [5] ile yönetilmesi mümkündür. Asimetrik şifreleme, işlem ve donanım karmaşıklığı nedeniyle tüketilen güç, etiket boyutu ve maliyeti simetrik şifrelemeye göre belirgin bir şekilde daha yüksektir. RFID etiketlerindeki güç/enerji kısıtlamaları göz önüne alarak pratik çözümler sunan asimetrik şifrelemeli çalışmalar aşağıda özetlenmiştir.

Eliptik eğri kriptografi (elliptic curve cryptography, ECC), RSA (Rivest-Shamir-Adelman) vb. diğer asimetrik şifreleme yöntemlerine göre daha küçük anahtar boyutu ile aynı sevi-

yede güvenlik sağlanmaktadır [5]. Bu nedenle ECC yöntemi, RFID etiketleri gibi donanımsal kısıtlamaları olan elektronik cihazlarda kullanımı yaygınlaşmaktadır [13]-[14]. [15]'te, RFID etiketleri için ECC algoritmasının kullanıldığı, güvenli ve etkin bir karşılıklı doğrulama protokolü geliştirilmiştir. Geliştirilen protokol sayesinde konum gizliliği (location privacy), iletim gizliliği (forward secrecy), ortadaki adam, taklit ve fiziksel saldırılara karşı önlem sağlandığı gösterilmiştir [15]. [16]'da, RFID etiketleri için çevrim-dışı kimlik doğrulamasının yapıldığı, ECC-tabanlı bir doğrulama protokolü geliştirilmiştir. Protokolde RFID etiketi ve okuyucusu arasında veri iletimi gerçekleşmeden önce çevrim-dışı (sunucuya bağlanmadan) karşılıklı doğrulama gerçekleştirilmektedir. Böylece yalnızca yetkili bir RFID okuyucusu etiketin içerisindeki bilgilere erişebilmektedir. Protokolün bazı önemli aktif ve pasif saldırılara karşı koruma sağladığı gösterilmiştir [16].

ECC, RSA algoritmasına göre daha düşük anahtar boyutu ile aynı güvenlik seviyesi sağlamakla birlikte, donanımsal karmaşıklığı AES algoritmasına göre yüksektir (bkz. Tablo 1, [7]). Düşük donanımsal karmaşıklıkla hızlı şifreleme, aynı zamanda güvenli anahtar paylaşımı yapabilmek için simetrik ve asimetrik kriptografi tekniklerinin bir arada kullanıldığı hibrid yöntemler tercih edilebilir [17]. Hibrid yönteme göre, RFID etiketinde AES, vb. simetrik anahtarlı şifreleme tekniği kullanılarak RFID etiketi ve okuyucu/sunucu arasında güvenli veri iletişimi sağlanır. Ayrıca, ECC vb. bir asimetrik anahtarlı kriptosistem ile PKI geliştirilerek güvenli anahtar paylaşımı yapılır. Tablo 1'deki "eşdeğer anahtar boyutu", sabit bir AES simetrik anahtar boyutu için ECC ve RSA algoritmalarında aynı düzeyde güvenlik sağlayan ve National Institute of Standards and Technology (NIST) enstitüsü tarafından belirlenen açık anahtar boyutları belirtilmektedir [18]-[19].

Algoritma	**ECC**	**RSA**	**AES**
İşlem hızı	Hızlı	Yavaş	Hızlı
Eşdeğer anahtar boyutu (ECC/RSA anahtar boyutu)	163 bit 256 bit 384 bit	1024 bit (1:6) 3072 bit (1:12) 7680 bit (1:20)	- 128 bit 192 bit
Eşdeğer imza boyutu (100 bitlik mesaj için)	321 bit (160 bit ECC)	1024 bit (1024 bit RSA)	-
Anahtar paylaşımı güvenliği	Yüksek	Yüksek	Düşük
Donanımsal işlem karmaşıklığı (512 bitlik sayıların mod. çarpımı için)	Yüksek (100,000 transistör)	Orta (50,000 transistör)	Düşük

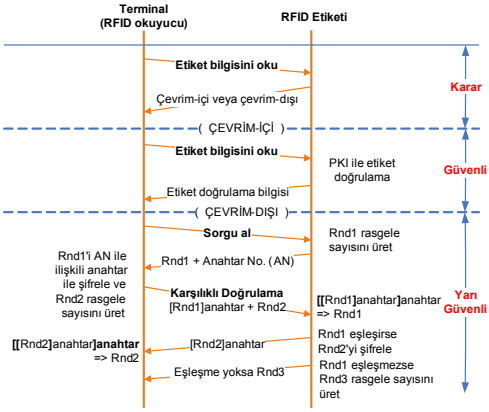
Tablo 1. ECC, RSA ve AES algoritmalarının karşılaştırılması

4. RFID Etiketinde Kademeli Güvenlik

PKI altyapısı, RFID etiketlere ait anahtarları güvenli bir şekilde paylaştırmak, anahtarlara kolay erişim sağlamak ve doğrulama yapmak için kullanılabilir. Doğrulama işlemi RFID okuyucusunda veya sunucuda (bkz. Şekil 2) yapılabilir. PKI ile RFID etiketinin kimlik doğrulamasında izlenen yöntem şu şekildedir. Etiket için özel ve açık anahtar ikilisi oluşturulur ve özel anahtar kullanılarak bir sayısal imza oluşturulur. Sayısal imza, etiketin ve sunucuda etikete ait sayısal sertifikanın içerisinde saklanır. Sayısal sertifika, etikete ait açık anahtar ile ilişkilendirilir. Etikete ait açık anahtar, etiketin doğrulanmasında kullanılır [20].

Terminal ve RFID etiketi arasında oluşan iletişim ve kararlar dizisinin işlem akışı Şekil 3'te göstermektedir. Kademeli güvenlik olarak tanımladığımız bu teknik, PKI altyapısı ile birlikte simetrik yöntemin de çevrim-dışı olarak kullanılması için tasarlanmış bir tekniktir. Bu işlem için terminal, RFID etiketin içerisindeki bilgiyi okuduktan sonra etiket doğrulamada gerekli olan güvenlik seviyesine ve/veya sunucu ile bağlantı olup olmamasına bağlı olarak

çevrim-içi veya çevrim-dışı işlem yapmaya karar verir. Sunucu ile bağlantı olması durumunda ve üst düzeyde güvenlik gerekiyorsa etiketin içerisindeki sertifika, PKI altyapısı ile sunucu üzerinde doğrulanır. Eğer daha düşük seviyede güvenlik yeterli ise, RFID etiketi çevrim-dışı olarak doğrulanır. RFID etiketi içerisinde simetrik veya asimetrik anahtarlı kriptografik bileşen bulunmasına bağlı olarak doğrulama işlemi değişiklik arz etmektedir. Çevrim-dışı doğrulama, simetrik anahtarlı kriptografik bileşen kullanılması durumunda, RFID etiketi içerisinde simetrik anahtarların listesi tutulur (örneğin 8 adet), şifrelemede kullanılacak anahtar rastgele olarak yonga tarafından atanır ve doğrulama Şekil 3'teki işlem akışına göre doğru ve yanlış ürün veya terminal kararları verilir.



Şekil 3. RFID etiketinde kademeli güvenlik

5. Sonuç ve Öneriler

RFID etiketlerindeki donanımsal, güç tüketimi, işlem gecikme süresi, maliyet ve boyut konusundaki kısıtlamalar nedeniyle etiketlerde maliyet, başarım ve güvenlik arasında ödünleşim bulunmaktadır. Düşük maliyetli RFID etiketleri için bu ödünleşimin en iyi şekilde yapılabilmesi için kriptosistem seçimi büyük önem arz etmektedir. RFID etiketindeki donanımsal (güç tüketimi, fiziksel boyut, işlem karmaşıklığı, işlem gecikme süresi, vb.) kısıtlamalardan dolayı simetrik anahtarlı kriptografiye dayalı kimlik doğrulama tercih edilen bir yöntemdir. Simetrik anahtarlı şifrelemede kullanılacak anahtarların daha güvenli bir şekilde paylaşılabilmesi için PKI altyapısı ile birlikte kullanılması tercih edilebilir. PKI altyapısında RFID etiket doğrulaması, güvenlik ihtiyacına göre çevrim-içi (sunucuda) veya çevrim-dışı (RFID okuyucusunda) yapılabilir. Örneğin, AES kripto-işlemcili bir RFID etiketi ve ECC algoritmalı bir PKI altyapısı ile düşük işlem gücüne sahip RFID etiketlerinde çevrim-içi doğrulama yapılarak yüksek güvenlik sağlanabilir.

5. Kaynaklar

[1] Glover, B. and Bhatt, H., RFID Essentials (1st ed.), **O'Reilly** (2006).

[2] Finkelzeller, K., The RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication (3rd ed.), **John Wiley &, Sons** (2003).

[3] "RFID Security and Privacy White Paper", RFID Feasibility Study Final Report, Attachment E, **Smart Border Alliance**, 2005.

[4] Hızlı Geçiş Sistemi (HGS), www.hgsmusteri.com.

[5] Stallings, W., Cryptography and Network Security: Principles and Practice (5th ed.), **Prentice Hall**, (2011).

[6] Juels, A., Blundo, C. and Cimato, S., "Minimalist Cryptography for Low-Cost RFID Tags", Proc. 4th International Conference on Security Communication Networks, 3352: 149 -164, **Springer-Verlag**, 2004.

[7] Eisenbarth, T., Kumar, S., "A Survey of Lightweight-Cryptography Implementations", **IEEE Design and Test of Computers**, 24 (6): 522-533, Nov.-Dec. 2007.

[8] Maimut, D., Ouafi, K., "Lightweight Cryptography for RFID Tags", **IEEE Security & Privacy**, 10 (2): 76-79, March-April 2012.

[9] Cole, P. H. and Ranasinghe, D. C., Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting (1st ed.), **Springer-Verlag**, (2008).

[10] Feldhofer, M., Dominikus, S. and Wolkerstorfer, J., "Strong Authentication for RFID Systems Using the AES Algorithm", **Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2004**, 3156: 357-370, Cambridge, MA, USA, August 2004.

[11] Toiruul, B. and Lee, K., "An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems", **International Journal of Computer Science and Network Security (IJCSNS)**, 6 (9B), 2006.

[12] Pham, T. A., Hasan, M. S. and Yu, H., "A RFID mutual authentication protocol based on AES algorithm", **UKACC International Conference on Control (CONTROL) 2012**, 997-1002, 3-5 September 2012.

[13] Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., Verbauwhede, I., "Public-Key Cryptography for RFID-Tags", **Proc. of IEEE International Conference on Pervasive Computing and Communications (PerCom) 2007,** 217–222 (2007).

[14] Hutter, M., "RFID Authentication Protocols Based on Elliptic Curves: A Top-Down Evaluation Survey", **International Conference on Security and Cryptography** (SECRYPT) 2009, 101-110, July 2009.

[15] Chou, J.-S., Chen, Y., Wu, C.-L., Lin, C.-F., "An efficient RFID mutual authentication scheme based on ECC", Report 2011/418, Cryptology ePrint Archive, 2011.

[16] Ahamed, S. I., Rahman, F., Hoque, M. E., "ERAP: ECC based RFID Authentication Protocol", 12th IEEE International Workshop on Future Trends of Distributed Computing Systems 2008 (FTDCS '08), 219-225, October 2008.

[17] JunLi, C., Dinghu, Q., Haifeng, Y., Hao, Z., Nie, M., "Email Encryption System Based on Hybrid AES and ECC", IET International Communication Conference on Wireless Mobile and Computing (CCWMC 2011), 347-350, November 2011.

[18] Barker, E., Johnson, D. and Smid, M., "NIST Special Publication 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)", **NIST**, March 2007.

[19] Barker, E., Chen, L., Regenscheid, A., and Smid, M., "NIST Special Publication 800-56B: Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography", **NIST**, August 2009.

[20] Başak, M., Adalı, E., "Akıllı Kartlar için Dinamik Güvenlik İşlevi", Bilgisayar Bilimleri ve Mühendisliği dergisi, **Türkiye Bilişim Vakfı**, Nisan 2012.