EK-3

ÖZGEÇMİŞ

1. Adı Soyadı : Aslı BAY
2. Doğum Tarihi : 20.09.1984
3. Unvanı : Dr. Öğr. Üy.
4. Öğrenim Durumu : Doktora
5. Çalıştığı Kurum : Antalya Bilim Üniversitesi

Derece	Alan	Üniversite	Yıl
Lisans	Matematik	Orta Doğu Teknik Üniversitesi	2007
Yüksek Lisans	Uygulamalı Matematik	Orta Doğu Teknik Üniversitesi	2009
Doktora	Bilgisayar ve Kominikasyon Bilimleri	Ecole Polytechnique Fédérale de Lausanne (EPFL)	2014

6. Akademik Unvanlar

Yardımcı Doçentlik Tarihi : Eylül 2020

7. Yayınlar

7.1. Uluslararası hakemli dergilerde yayınlanan makaleler (SCI,SSCI,Arts and Humanities)

7.1.1. Aslı Bay, Atefeh Mashatan and Serge Vaudenay, Revisiting Iterated Attacks in the Context of Decorrelation Theory. The Journal of Cryptography and Communications Discrete Structures, Boolean Functions and Sequences (CCDS), volume 6, pages 279–311, 2014.

7.3. Uluslararası bilimsel toplantılarda sunulan ve bildiri kitabında basılan bildiriler

7.3.1. Aslı Bay, Oğuzhan Ersoy ve Ferhat Karakoç, Universal Forgery and Key Recovery Attacks on ELmD Authenticated Encryption Algorithm. 22nd International Conference onthe Theory and Application of Cryptography and Information Security in Vietnam (ASIACRYPT 2016), volume 10031 of LNCS, pages 354-368, 2016.

7.3.2. Aslı Bay, Celine Blondeau ve Serge Vaudenay, Protecting against Multidimensional Linear and Truncated Differential Cryptanalysis by Decorrelation. 22nd International Workshop on Fast Software Encryption (FSE 2015), volume 9054 of LNCS, pages 73-91, Springer, 2016.

7.3.3. Aslı Bay, Jialin Huang ve Serge Vaudenay, Improved Linear Cryptanalysis of Reduced-Round MIBS. The 9th International Workshop on Security (IWSEC 2014), volume 8639 of LNCS, pages 204-220, Springer, 2014.

7.3.4. Aslı Bay, Atefeh Mashatan ve Serge Vaudenay, Resistance Against Adaptive Plaintext-Ciphertext Iterated Distinguishers. The 13th International Conference on Cryptology in India (INDOCRYPT 2012), volume 7668 of LNCS, pages 528-544, Springer, 2012.

7.3.5. Aslı Bay, Ioana Boureanu, Katerina Mitrokotsa, Iosif Daniel Spulber ve Serge Vaudenay. The Bussard-Bagga and Other Distance Bounding Protocols under Man-in-the-Middle Attacks. The 88th China International Conference on Information Security and Cryptology (INSCRYPT 2012), volume 7763 of LNCS, pages 371-391, Springer, 2012.

7.3.6. Aslı Bay, Atefeh Mashatan ve Serge Vaudenay, Resistance Against Iterated Attacks by Decorrelation Revisited. The 32nd International Cryptology Conference (CRYPTO 2012), volume 7417 of LNCS, pages 741-757, Springer, 2012.

7.3.7. Aslı Bay, Atefeh Mashatan ve Serge Vaudenay, A Related-Key Attack against Multiple Encryption based on Fixed Points. The 8th International Joint Conference on e-Business and Telecommunications (ICETE 2011), Communications in Computer and Information Science Berlin, Springer, 2011.

7.3.8. Aslı Bay, Jorge Nakahara ve Serge Vaudenay, Cryptanalysis of reduced-round MIBS Block Cipher (The Best Paper Award). The 10th International Conference on Cryptology And Network Security (CANS 2010), volume 6467 of LNCS, pages 1-19, Springer-Verlag, 2010.

7.6. Ulusal bilimsel toplantılarda sunulan ve bildiri kitabında basılan bildiriler

7.6.1. Ali Doğanaksoy, Aslı (Darbuka) Bay, Dilek (Özberk) Çelik, Neşe (Öztop) Koçak ve Fatih Sulak, A Survey of the Related-key Attacks on AES. The 3rd Information Security and Cryptology Conference with International Participation (ISC 2008), Türkiye, 2008.

7.6.2. Ali Doğanaksoy, Aslı (Darbuka) Bay, Dilek (Özberk) Çelik, Neşe (Öztop) Koçak ve Fatih Sulak, A Survey of the Attacks on AES. The 3rd Information Security and Cryptology Conference with International Participation (ISC 2008), Türkiye, 2008.

8.Projeler

8.1 European Project: The SECREDAS Project (Aralık 2018-Eylül 2020)

8.2 2232- Yurda Dönüş Burs Programı (Eylül 2015 – Eylül 2017): Proje Başlığı: CAESAR Doğrulanmış Şifreleme Algoritmalarının Kriptanalizi (No. 115C119)

9. İdari Görevler

Görev Unvanı	Görev Yeri
Siber Güvenlik Yüksek Lisans Programı Koordinatör	Lisansüstü Eğitim Enstitüsü

10. Bilimsel ve Mesleki Kuruluşlara Üyelikler

International Association for Cryptologic Research (IACR), (2008-halen).

11. Ödüller

1. “Cryptanalysis of reduced-round MIBS Block Cipher” adlı bildiri için en iyi makale ödülü: (International Conference on Cryptology and Network Security (CANS 2010)

12. Son iki yılda verdiğiniz lisans ve lisansüstü düzeydeki dersler için aşağıdaki tabloyu doldurunuz.

Akademik Yıl	Dönem	Dersin Adı	Haftalık Saati		Öğrenci Sayısı
			Teorik	Uygulama	
2020-2021	**Güz**	CS472 Kriptografi	Teorik	Uygulama	27
	İlkbahar				
2020-2021	**Güz**	CS411 Çizge Kuramı	Teorik		25
	İlkbahar				

Not: Açılmışsa, yaz döneminde verilen dersler de tabloya ilave edilecektir.