

CHES Workshop 10. Yıl

Geçtiğimiz hafta Cryptographic Hardware and Embedded Systems (kriptografik donanım ve yerleşik sistemler) konferansının onuncusu, Washington'da toplandı. 250 bilim



**ÇETİN KAYA
KOÇ**

adamı ve mühendisin katıldığı bu konferansı ben ve Christof Paar 1999 yılında Worcester Politeknik Enstitüsü'nde başlatmıştık. CHES konferansına her yıl yaklaşık 250 kişi katılıyor ve 120 kadar makale gönderiliyor. Onuncu yıl dolayısıyla geriye dönüp bir değerlendirme yapmak ve ileriye doğru bir iki söz söylemekte fayda görüyorum. Christof Paar ile birlikte kurucular ve yönetim kurulu sürekli üyeleri olarak bir değerlendirme yaptık aslında. Yazdığım bu görüşler ortak paydalar.

İlk söylenecek şey motivasyon ve başlatma nedenlerimiz. O zamanlar Crypto ve Eurocrypt gibi çok başarılı iki kriptografi konferansı varken, CHES'e neden gerek vardı? Sebebi açık aslında: Bu iki konferansta da kriptografinin donanım ve yazılım olarak gerçekleştirilmeleri hakkındaki makaleler bir veya iki taneyi geçmiyordu. Asıl konsantrasyonu algoritmalar, protokoller ve kriptanaliz olan bu konferanslarda gerçekleştirilecek makalelerine yeteri kadar

yer yoktu. Donanım ve yazılım ile ilgili başka konferansların program komiteleri ise kriptografiden habersiz oldukları için yapılan çalışmaları anlamıyorlar ve gereken ilgiyi gösteremiyorlardı.

Gereksinim nedenleri çok açık seçik olsa bile,

CHES konferansı başarılı olmayabilirdi. Bu kadar çok başarılı olmasının arkasında yatan en önemli neden, yan-kanal saldırıları (side-channel attacks) çalışmalarının doğuşunun CHES'in başlangıç yıllarına gelmesi ve bu makalelerin CHES'de kendilerine yer bulmasıydı. Eğer kurucular olarak kendimizi sadece uygulama algoritmaları, kriptografik donanım ve yazılım mimarileri ile sınırlı kılsaydık ve yan-kanal makalelerini dışarıya itseydik, CHES bu kadar başarılı olmazdı ve belki de yan-kanal saldırı ve saldırıya-karşı-tasarım (countermeasures) çalışmaları da bu kadar zenginleşmezdi. Bizim zaman içinde önyargıdan uzak olarak verdiğimiz bu kararın CHES'in ve yan-kanal çalışmalarının ortak başarısına en büyük katkı nedeni olarak görüyorum. CHES'in onuncu yılında konferansın başarısında itici güç olan bütün makale yazarlarını kutlarım. CHES'in başarısı size ait.

koc@cryptocode.net