به نام خدا

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه

منحرف کردن توابع بولی، و کاربرد آن در حمله به رمزنگاری مقاوم در برابر دستکاری

How to Bias Boolean Functions, and Applications to Attack Tamper-Resilient Cryptography

احمد بورقانی فراهانی (از طرف دکتر محمد محمودی)

زمان: شنبه ۲۰ مهرماه ۱۳۹۲، ساعت ۹:۰۰ صبح

مکان: دانشکده مهندسی کامپیوتر، طبقه پنجم، آزمایشگاه امنیت داده و شبکه

الگوریتم‌های رمزنگاری امروزی برای تأمین امنیت معنایی، که ساده‌ترین تعریف امنیت می‌باشد، می‌بایست الگوریتم‌های تصادفی باشند و از سیستم، مقادیری تصادفی را دریافت نمایند. در این ارائه، نشان داده می‌شود که اگر بتوان به گونه‌ای اعداد تصادفی تولید شده در سیستم را کمی تغییر داد، دیگر رمزنگاری امن ممکن نخواهد بود. به طور دقیق‌تر، اگر حمله‌کننده بتواند هر بیت از اعداد تصادفی تولید شده توسط سیستم برای استفاده در رمزنگاری را با احتمال p تغییر دهد، در این صورت هر الگوریتم رمزنگاری را می‌توان با احتمال $p/10$ شکست. در قلب این حمله، الگوریتمی کارا ارائه شده است که می‌تواند با تغییراتی در ورودی تصادفی هر تابع بولی، میانگین خروجی آن را به میزان قابل توجهی منحرف کند.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.