تقلیل حملهٔ بازهمزمان‌سازی به حملهٔ متمایزکننده علیه سیستم‌های رمز دنباله‌ای

آرش میرزایی[۱]، محمد دخیل علیان[۲] و محمود مدرس هاشمی[۳]
[۱]آزمایشگاه امنیت و رمزنگاری دانشگاه صنعتی اصفهان، arash_mirzaei@ec.iut.ac.ir
[۲]آزمایشگاه امنیت و رمزنگاری دانشگاه صنعتی اصفهان، mdalian@cc.iut.ac.ir
[۳] آزمایشگاه امنیت و رمزنگاری دانشگاه صنعتی اصفهان، modarres@cc.iut.ac.ir

چکیده – حملهٔ بازهمزمان‌سازی حمله‌ای از نوع بازیابی کلید است که در حالت کلی به ساختارهای دارای مقداردهی اولیه و به هنگام‌سازی خطی قابل اعمال می‌باشد. در این مقاله با استفاده از ایدهٔ حملهٔ بازهمزمان‌سازی حمله‌ای جدید از نوع متمایزکننده به این ساختارها ارائه می‌شود. در حملهٔ پیشنهادی سعی شده است تا با کاهش میزان کلید اجرایی و پیچیدگی محاسباتی مورد نیاز، حملهٔ بازهمزمان‌سازی به حملهٔ متمایزکننده تقلیل یابد. همچنین مثالی خاص از ساختارهای دارای مقداردهی اولیهٔ غیر خطی که پیش از این، حملهٔ بازهمزمان‌سازی به آن اعمال شده است نیز معرفی و حملهٔ متمایزکننده به آن پیشنهاد می‌شود.

کلید واژه- حملهٔ بازهمزمان‌سازی، حملهٔ متمایزکننده، رمزکنندهٔ دنباله‌ای، مقداردهی اولیه

۱- مقدمه

حملات به رمزکننده‌های قالبی تنها با هدف بازیابی تمام یا قسمتی از کلید انجام می‌شوند در حالیکه حملات به رمزکننده-های دنباله‌ای با فرض متن پیام معلوم با دو هدف زیر صورت می‌گیرند[۱]:

- بازیابی کلید که با هدف حصول تمام یا قسمتی از کلید انجام می‌گیرند.
- تمایز کلید اجرایی که با هدف متمایز نمودن دنبالهٔ کلید اجرایی از یک دنبالهٔ کاملاً تصادفی صورت می‌گیرند.

اگر چه حملات بازیابی کلید به وضوح، قوی‌ترین دسته از حملات می‌باشند و در واقع تحلیل‌گر را قادر به اعمال حملات متمایزکننده نیز می‌سازند ولی یک رمزکنندهٔ دنباله‌ای امن باید در مقابل حملات متمایزکننده نیز مقاوم باشد. حملات متمایزکننده امنیت بسیاری از سیستم‌های رمز دنباله‌ای ارائه شده به رقابت‌های NESSIE [۲] و eSTREAM [۳] را تهدید کرده‌اند.

در تحلیل یک مولد رمز دنباله‌ای، هدف از حملهٔ متمایزکننده یافتن شواهدی مبنی بر کاملاً تصادفی نبودن دنبالهٔ کلید اجرایی تولید شده توسط مولد می‌باشد[۴]. حملهٔ متمایزکننده را می‌توان به این ترتیب توصیف نمود که جعبهٔ سیاهی تحت عنوان متمایزگر[۱] وجود دارد که دنباله‌ای از سمبل-ها را به عنوان ورودی دریافت نموده و خروجی آن یکی از این دو پاسخ است "دنباله توسط مولد کلید اجرایی تولید شده است" یا "دنباله کاملاً تصادفی است". اگر متمایزگر بتواند با احتمالی مخالف ۰/۵ پاسخ صحیح دهد، حمله موفق است. در صورتیکه دنبالهٔ در دسترس از رمزکننده حاصل شده باشد ولی خروجی متمایزگر به اشتباه پاسخ "دنباله کاملاً تصادفی است" باشد خطای نوع اول یا خطای از دست دادن پاسخ[۲] حادث شده و اگر دنبالهٔ در دسترس کاملاً تصادفی باشد و خروجی متمایزگر اشتباه باشد خطای نوع دوم یا خطای هشدار کاذب[۳] رخ داده است.

حملهٔ بازهمزمان‌سازی[۴] از نوع بازیابی کلید و بردار اولیه (IV) انتخاب شده[۵] است و در حالت کلی به رمزکننده‌هایی با مقداردهی اولیه و به‌هنگام‌سازی خطی قابل اعمال است[۵]،[۶].

[1] -Distinguisher
[2] -Miss
[3] -False Alarm
[4] -Resynchronization Attack
[5] -Chosen IV