به نام خدا

محمد سعید صدیقی

محمد صادقی

(a

اگر کلید ها تغییر نکنند مشخصا در صورت افشا شدن کلید ها نه مکالمات گذشته و نه مکالمات آینده امن خواهند بود و همگی قابل رمزگشایی هستند زیرا ما همه کلید های مورد نیاز به علاوه iv اولیه را داریم و میتوانیم همه chain key ها را از ابتدا بسازیم. پس نه Forward Secrecy داریم و نه Break-in Recovery.

(b

برای آلیس طول بلند ترین زنجیره ۲ و برای باب ۱ است. زیرا به محض دریافت پیام از طرف مقابل کلید ها ما تغییر میکنند و در نتیجه زنجیره از اول شروع می شود. پس آلیس در دو پیام اول به طول زنجیر ۲ میرسد و بعد از اول پیام باب کلید های جدید تولید می شوند.

(c

به این ویژگی Forward Secrecy می گویند که یعنی حتی اگر در مرحله ای تمام کلید ها افشا شوند پیام ها رد و بدل شده در گذشته قابل رمزگشایی نیستند.

در Double Rachet ما مدام در حال تغییر کلید ها برای رمز کردن پیام هستیم پس اگر در مرحله ای کلید افشا شود کلید مرحله قبلی و قبل تر قابل بازیابی از کلید افشا شده نیستند. (هم کلید رمز پیام و هم کلید های session مدام تغییر میکنند)

(d

- زمان بیشتر برای تولید کلید: معمولا RSA
- زمان بیشتر برای تولید امضا: RSA

- طول امضا: طول امضا های ECDSA کمتر است با امنیت یکسان (طول امضای RSA ثابت و طول امضای ECDSA متغییر است.)
- زمان مورد نیاز برای تایید امضا: RSA زمان بیشتری برای تایید امضا نیاز دارد.