Cryptology ePrint Archive: Report 2011/688

Authenticated Key Exchange under Bad Randomness

Guomin Yang and Shanshan Duan and Duncan S. Wong and Chik How Tan and Huaxiong Wang

Abstract: We initiate the formal study on authenticated key exchange (AKE) under bad randomness. This could happen when (1) an adversary compromises the randomness source and hence directly controls the randomness of each AKE session; and (2) the randomness repeats in different AKE sessions due to reset attacks. We construct two formal security models, Reset-1 and Reset-2, to capture these two bad randomness situations respectively, and investigate the security of some widely used AKE protocols in these models by showing that they become insecure when the adversary is able to manipulate the randomness. On the positive side, we propose simple but generic methods to make AKE protocols secure in Reset-1 and Reset-2 models. The methods work in a modular way: first, we strengthen a widely used AKE protocol to achieve Reset-2 security, then we show how to transform any Reset-2 secure AKE protocol to a new one which also satisfies Reset-1 security.

Category / Keywords: cryptographic protocols / Authenticated Key Exchange, Resettable Cryptography, Bad Randomness

Publication Info: FC 2011

Date: received 18 Dec 2011

Contact author: tslyg at nus edu sg

Available formats: PDF | BibTeX Citation

Version: 20111223:121339 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]