The Exact Security of Full Domain Hash Signature Schemes

Tan Syh Yuan

Faculty of Information Science and Technology
Multimedia University
sytan@mmu.edu.my

Abstract

In 1993, Bellare and Rogaway proposed a generic technique to construct a signature scheme, namely, full domain hash (FDH) signature scheme. They gave a RSA instantiation, namely, RSA-FDH signature scheme and showed that the probability ϵ of breaking RSA-FDH in time t is $(q_{hash}+q_{sig})\epsilon'$ where ϵ' is the probability of solving RSA problem in time t' while q_{hash} and q_{sig} are respectively the total hash and sign queries issued by the forger. Subsequently, they introduced the methodology of quantifying the security reduction by interpreting the security tightness based on the ratio of $t\epsilon$ versus $t'\epsilon'$. If the ratio is close to 1, it is termed as a tight reduction, else it is a loose reduction. We will discuss the techniques emerged along the way to discover the exact security of FDH signature, starting from the index guessing, to coin tossing, salting and finally the selector bit.