Cryptology ePrint Archive: Report 2013/168

On secure embedded token design (Long Version) -- Quasi-looped Yao circuits and bounded leakage

Simon Hoerder and Kimmo Järvinen and Dan Page

Abstract: Within a broader context of mobile and embedded computing, the design of practical, secure tokens that can store and/or process security-critical information remains an ongoing challenge. One aspect of this challenge is the threat of information leakage through side-channel attacks, which is exacerbated by any resource constraints. Although any countermeasure can be of value, it seems clear that approaches providing robust guarantees are most attractive. Along these lines, this paper extends previous work on use of Yao circuits via two contributions. First, we show how careful analysis can fix the maximum number of traces acquired during a DPA attack, effectively bounding leakage from a Yao-based token: for a low enough bound, the token can therefore be secured via conventional (potentially less robust) countermeasures. To achieve this we use modularised Yao circuits, which also support our second contribution: the first Yao-based mplementation of a secure authentication payload, namely HMAC based on SHA.

Category / Keywords: implementation / Yao circuits, side-channel attacks, leakage-resilient, mobile/embedded tokens, AES, HMAC, SHA

Publication Info: Workshop on Information Security Theory and Practice (WISTP) 2013

Date: received 22 Mar 2013

Contact author: hoerder at cs bris ac uk