

Why CHES is better than CRYPTO¹

Daniel J. Bernstein and Tanja Lange

2010.08.19

¹Except for the rump session

Coffee break at CRYPTO



Coffee break at CHES



Coffee break at CHES



Audience at CRYPTO



Audience at CHES



CRYPTO has talks on leakage resilience ...

CRYPTO has talks on leakage resilience ...



... but fails to achieve it



... but fails to achieve it



CHES to the rescue



CHES does not leak!



CRYPTO vs. CHES

(Loading 3906.avi)