Why CHES is better than CRYPTO[1]

Daniel J. Bernstein and Tanja Lange

2010.08.19

[1] Except 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!