Optimal Key Ranking for Side-Channel Attacks

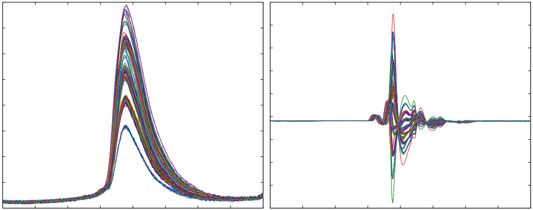
N. Veyrat-Charvillon, B. Gérard,
M. Renauld and F-X. Standaert

UCL Crypto Group, Université catholique de Louvain

CHES 2011, September 30

Standard DPA Attacks

Side-channel traces



Standard DPA Attacks

$$\boxed{\text{Side-channel traces}} \downarrow \boxed{\text{some kind of statistics}}$$

$$\rho_{X,Y} = \frac{\mathrm{cov}(X,Y)}{\sigma_X \sigma_Y}$$

Standard DPA Attacks

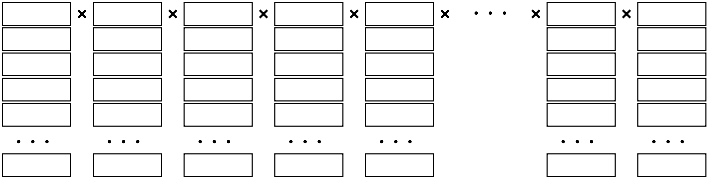
Side-channel traces

↓

some kind of statistics

↓

rank subkeys



Standard DPA Attacks

Side-channel traces

↓

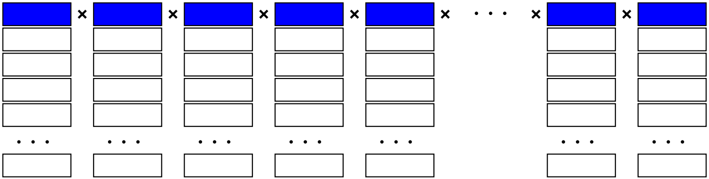
some kind of statistics

↓

rank subkeys

↓

output key(s)



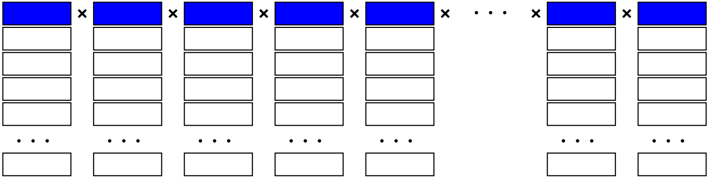
Key is incorrect !

Abort, Retry, Fail ?

Let's try again

Output another key, or two, or 2^{32} !

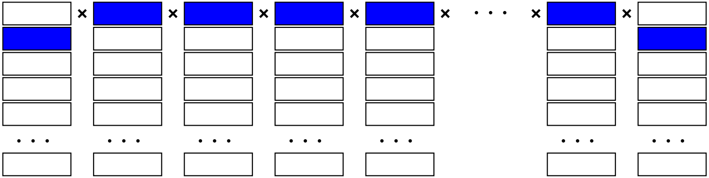
Wait. . . how do we choose them ?



Let's try again

Output another key, or two, or 2^{32} !

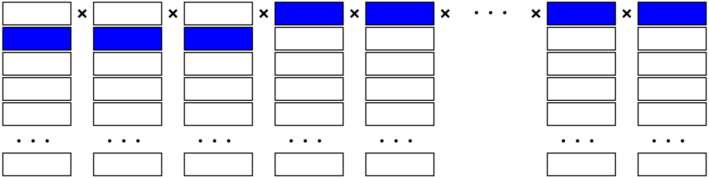
Wait. . . how do we choose them ?



Let's try again

Output another key, or two, or 2^{32} !

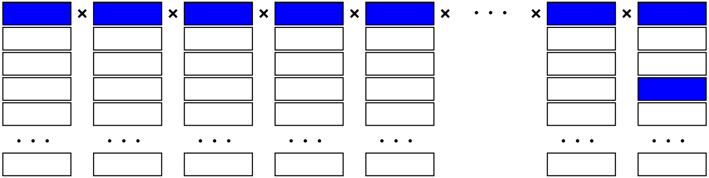
Wait... how do we choose them ?



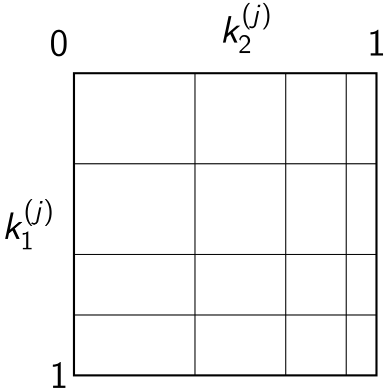
Let's try again

Output another key, or two, or 2^{32} !

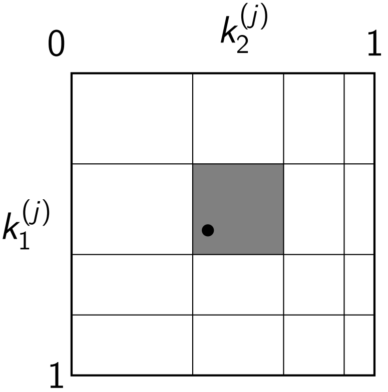
Wait. . . how do we choose them ?



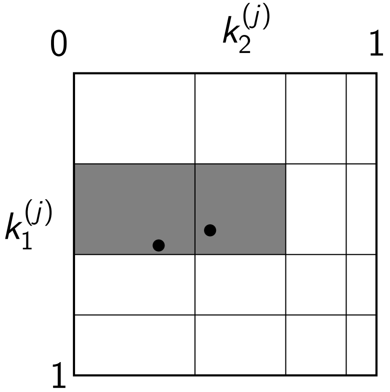
Random sampling: EUROCRYPT '91



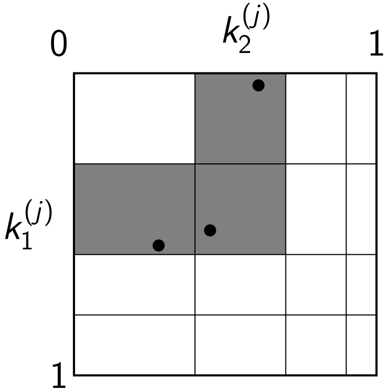
Random sampling: EUROCRYPT '91



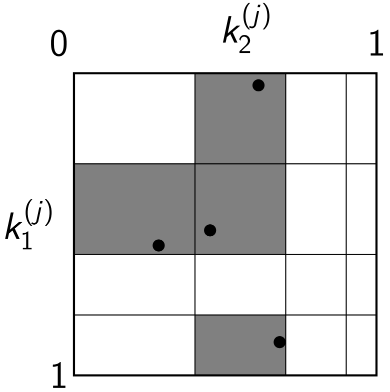
Random sampling: EUROCRYPT '91



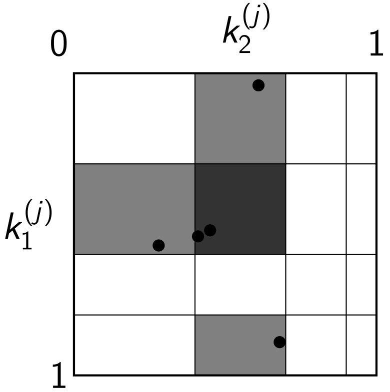
Random sampling: EUROCRYPT '91



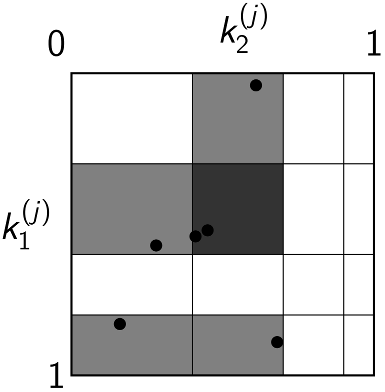
Random sampling: EUROCRYPT '91



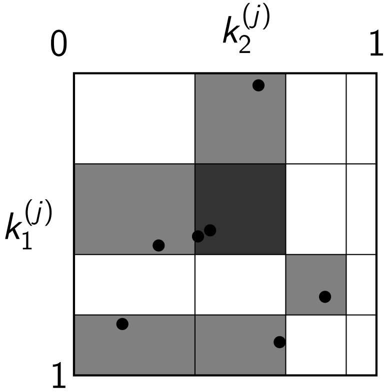
Random sampling: EUROCRYPT '91



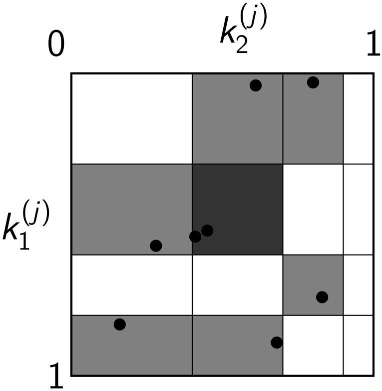
Random sampling: EUROCRYPT '91



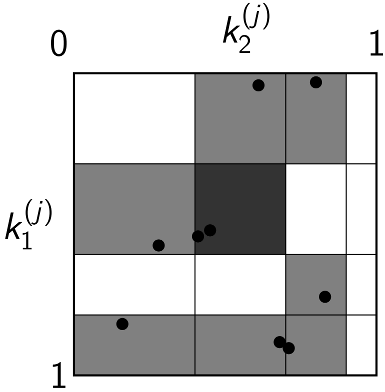
Random sampling: EUROCRYPT '91



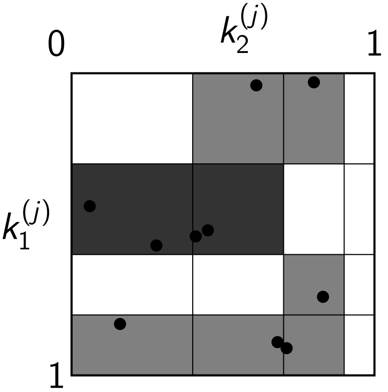
Random sampling: EUROCRYPT '91



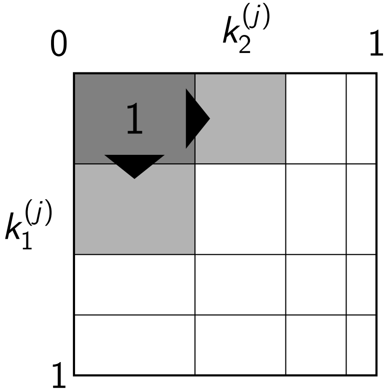
Random sampling: EUROCRYPT '91



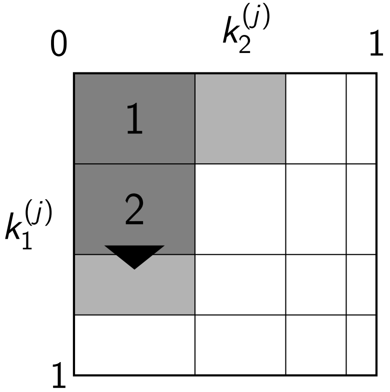
Random sampling: EUROCRYPT '91



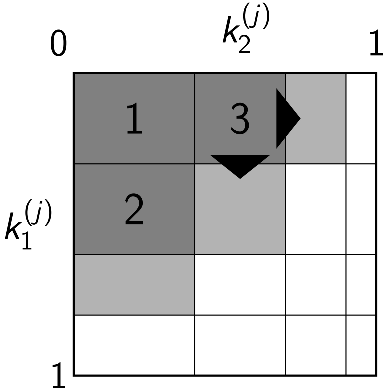
Optimal enumeration



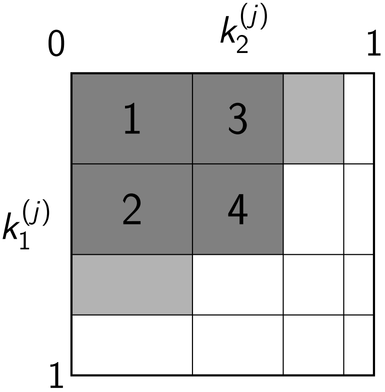
Optimal enumeration



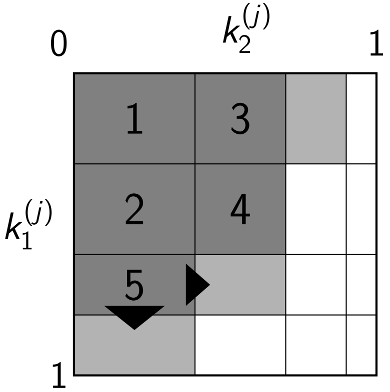
Optimal enumeration



Optimal enumeration

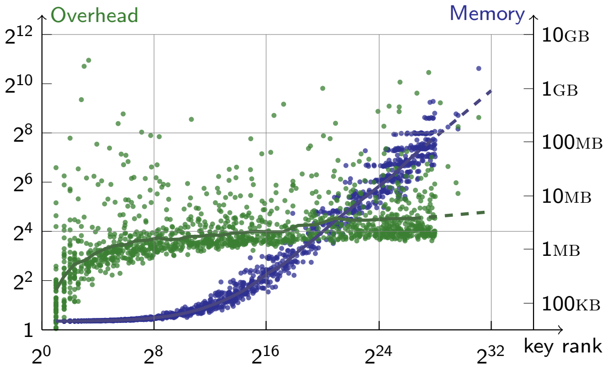


Optimal enumeration

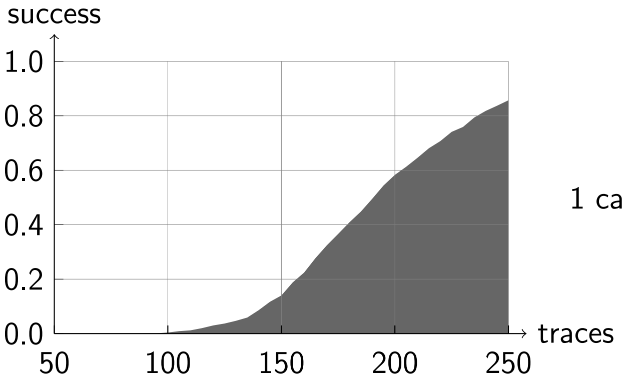


Sampling overhead

#Trials	2^{16}	2^{20}	2^{24}	2^{28}	2^{32}	2^{36}	2^{40}
Sampling	0.04s	0.31s	10.1s	160s	2560s	11h	182h
Enumeration	0.03s 405KB	0.55s 2.7MB	9.2s 20MB	163s 225MB	3130s 1.8GB	12h 10GB	221h 70GB

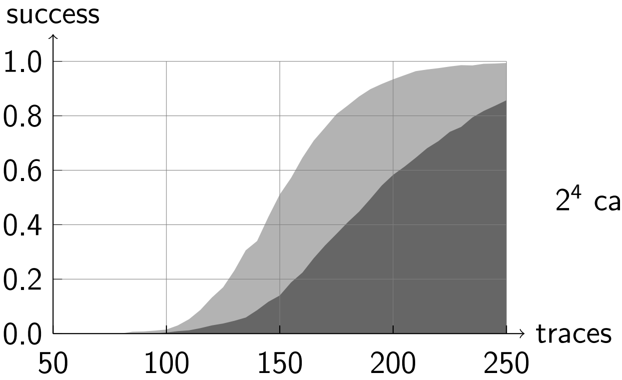


Success rate: optimal enumeration



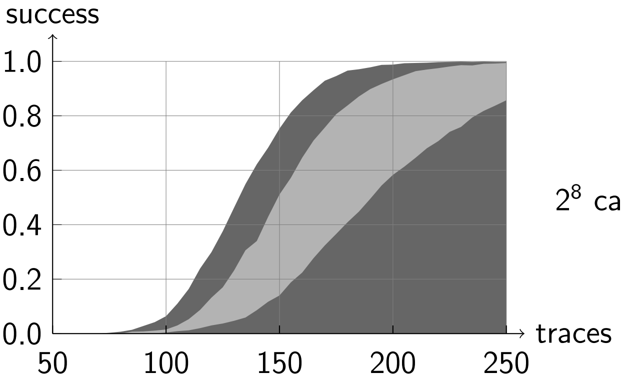
1 candidate

Success rate: optimal enumeration



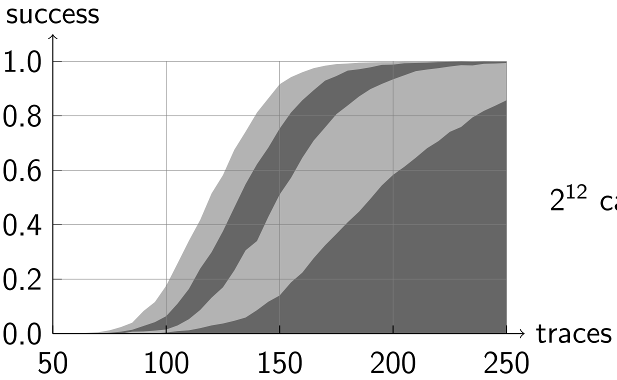
2^4 candidates

Success rate: optimal enumeration



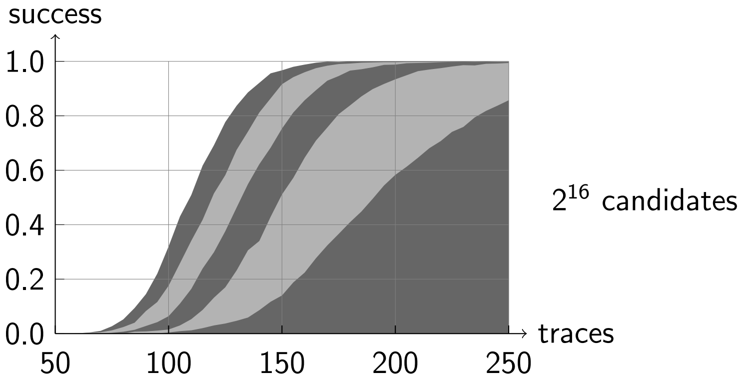
2^8 candidates

Success rate: optimal enumeration

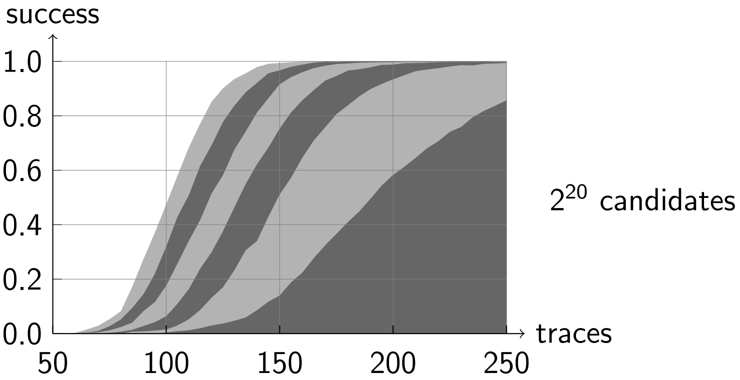


2^{12} candidates

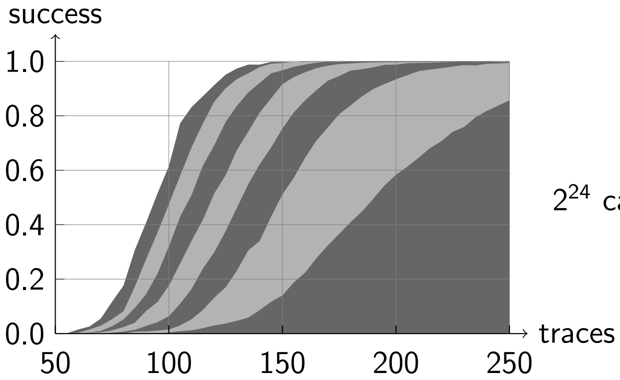
Success rate: optimal enumeration



Success rate: optimal enumeration

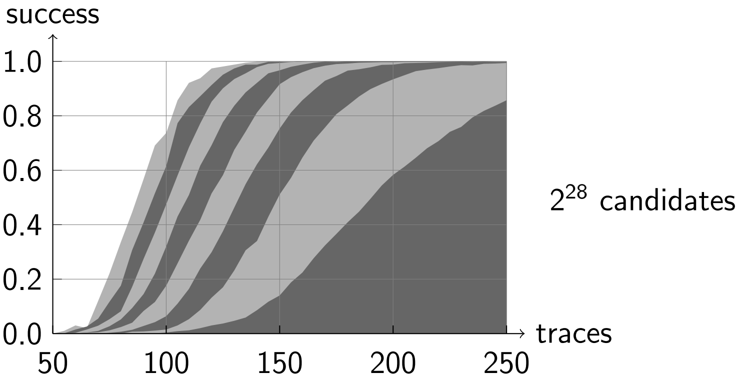


Success rate: optimal enumeration

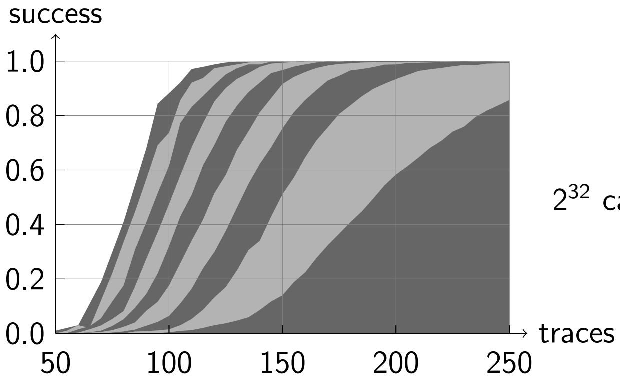


2^{24} candidates

Success rate: optimal enumeration



Success rate: optimal enumeration



2^{32} candidates

If at first you don't succeed ...

http://eprint.iacr.org/2012/???