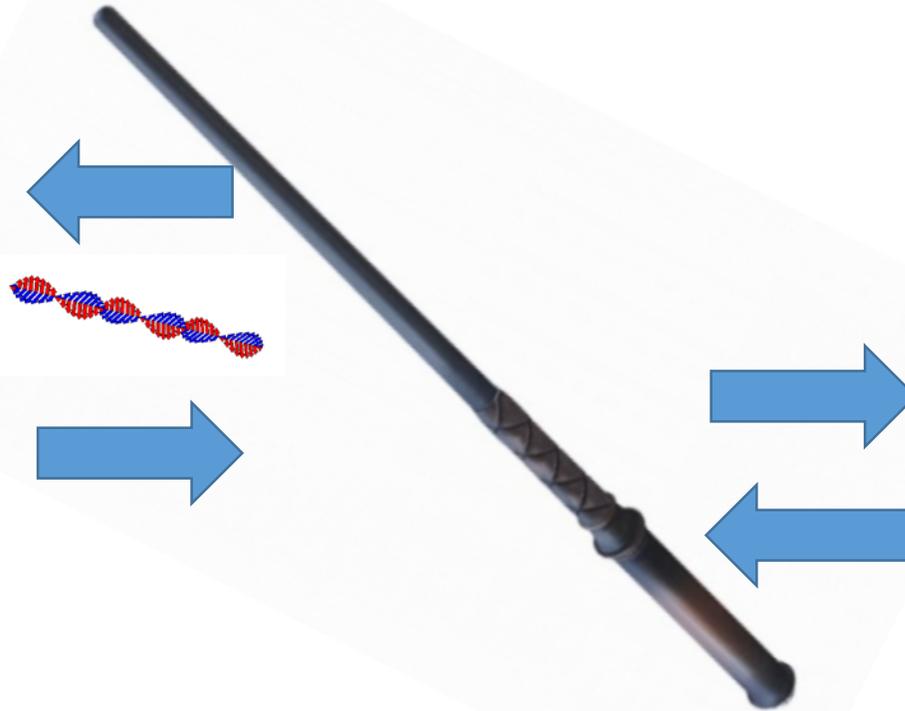


EM-Side-Channel Resistant Symmetric-Key Authentication Mechanism for Small Devices

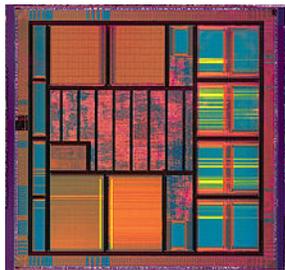
Boivie, Jutla, Friedman, Shahidi

IBM T.J. Watson Research Center

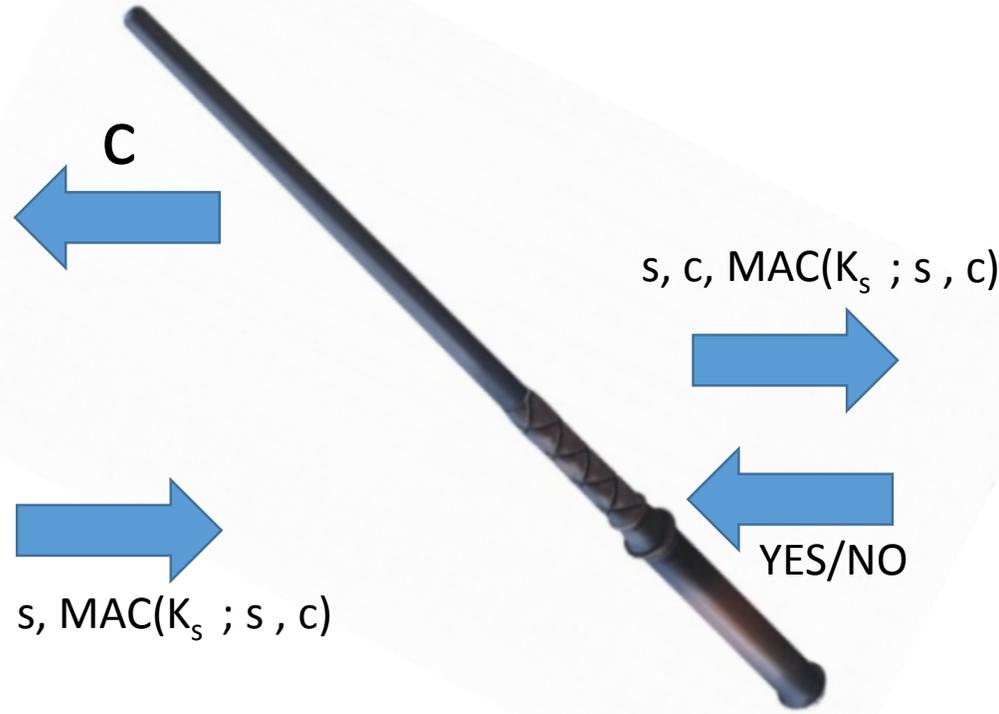
Authenticating Bank Notes



Authenticating Bank Notes



Serial No. s
Secret K_s



Serial No. s
Secret K_s

Storing Secret Keys in 14nm and Beyond

- Once written, the keys can only be accessed through built-in circuitry.
- Not possible to read through electron microscopy or ion beams
 - (at least current technology)
- **Electromagnetic Radiation Leakage still a concern**
 - During processing of the secret key there is EM leakage
 - Gate specific leakage
 - Aggregate leakage over carrier frequency
 - Similar to power usage leakage

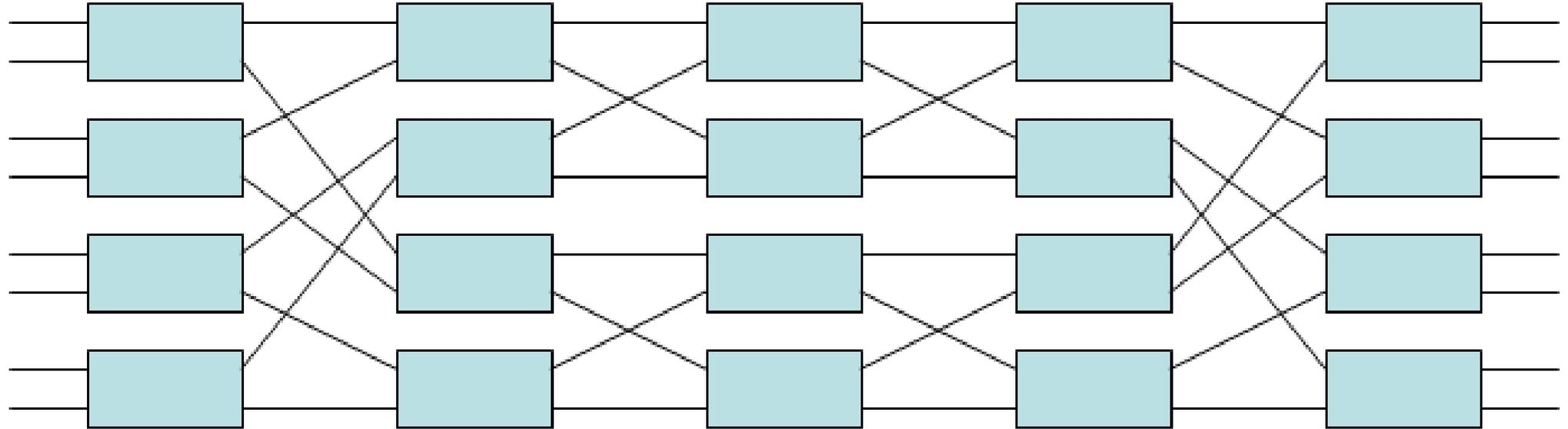
Traditional Countermeasure

1. Use Public Key Cryptography to authenticate challenge
 - Limits the number of samples for EM attack
 2. Or, expensive randomized secret-shared processing of each step
 - Reduces the differential attack signal
- Both require RNG on chip.
 - Public-key solution requires chip to generate a random nonce first.
 - Otherwise replay of challenge possible
 - Rather expensive to implement, and still not adequate.

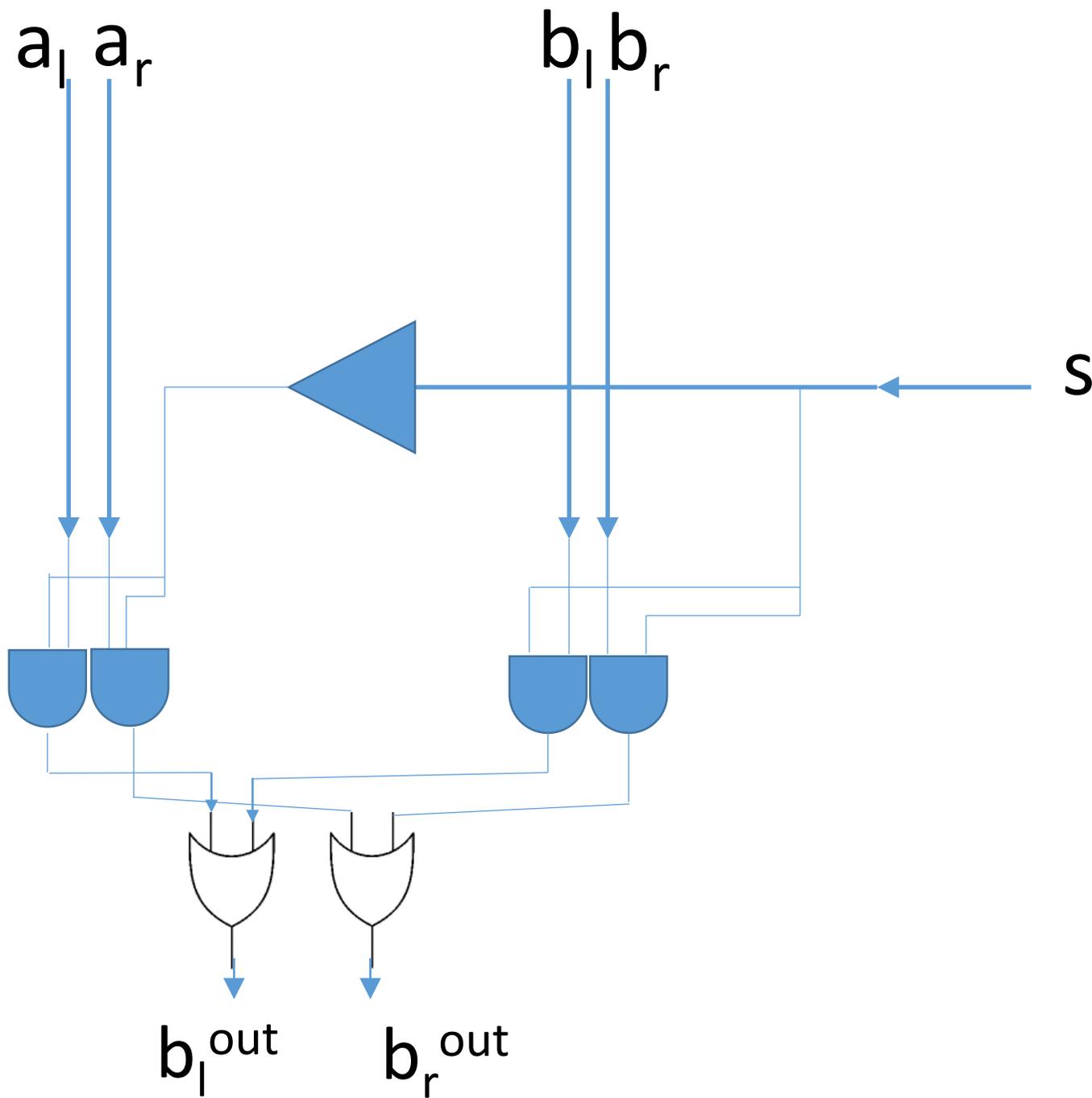
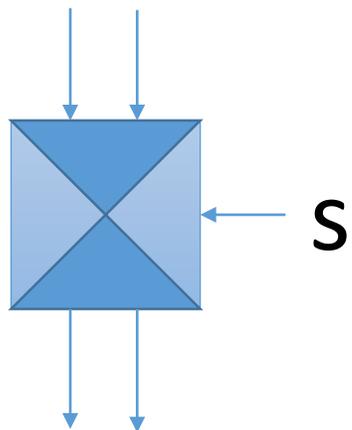
Novel Solution based on Benes Network

- Use challenge c to generate a permutation of 128 bits
- **Permute the 128 bit secret K_S .**
- MAC using the permuted secret.
- Server also computes the same permutation (from c).
 - Computes the MAC with the same permuted secret.
- **Also encode each bit of secret using two bits**
 - 0 encoded as 01 and 1 encoded as 10

Benes Permutation Network



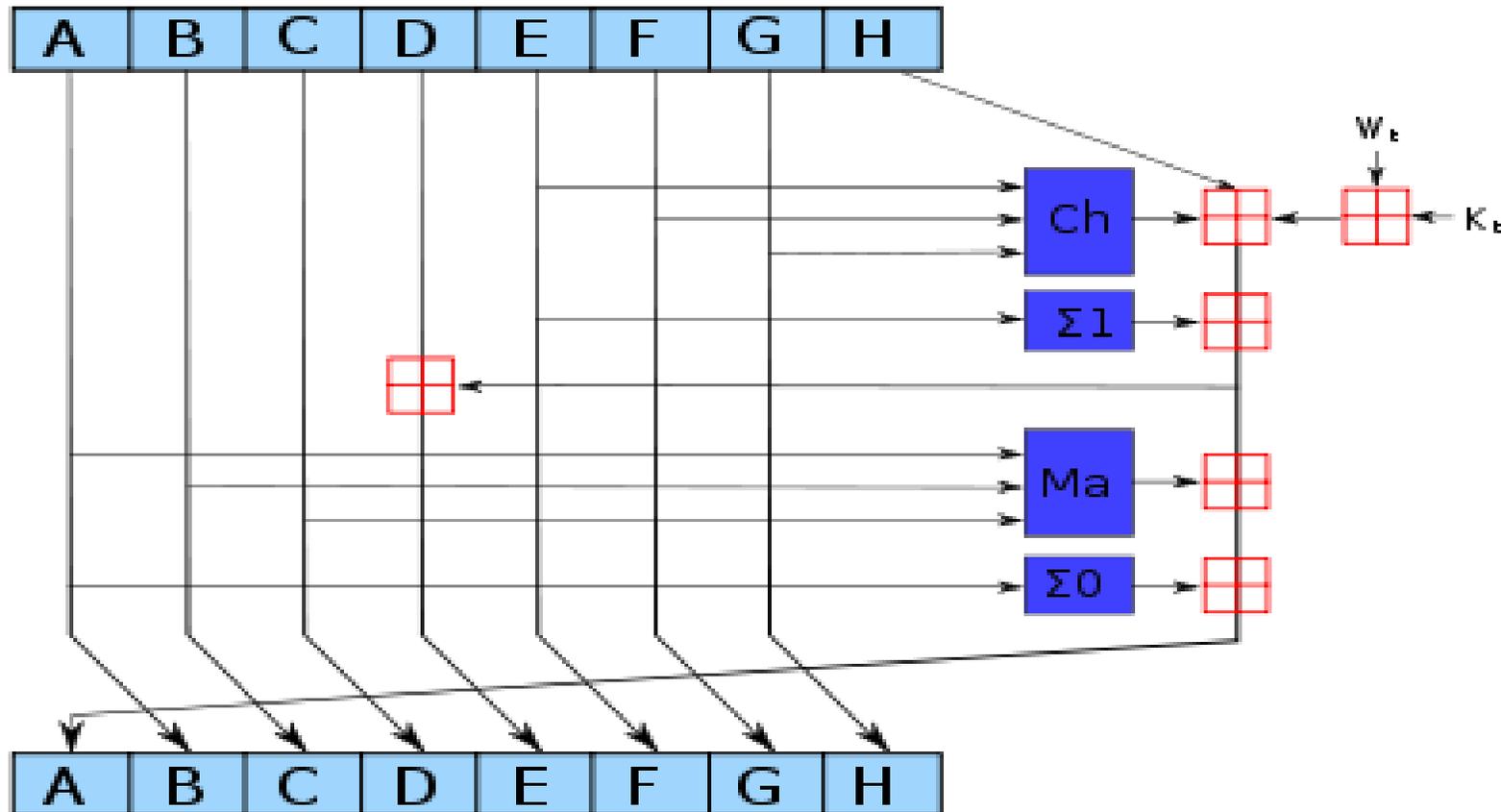
2 X 2 Switch



Probability of same 8 bits of secret key showing up at W_t is $120!/128!$

Which is 2^{-50}

$$\Delta = 00000001$$



THANKS!