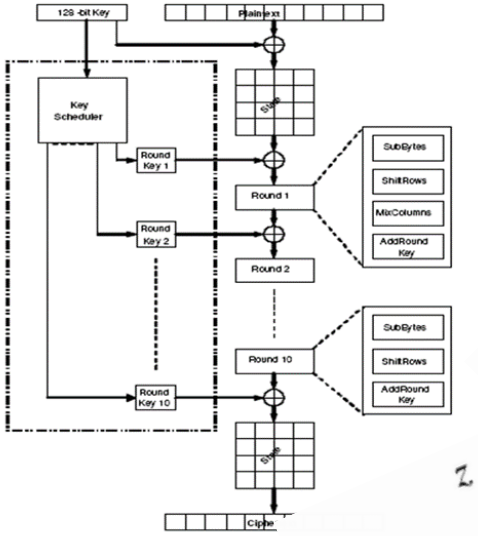
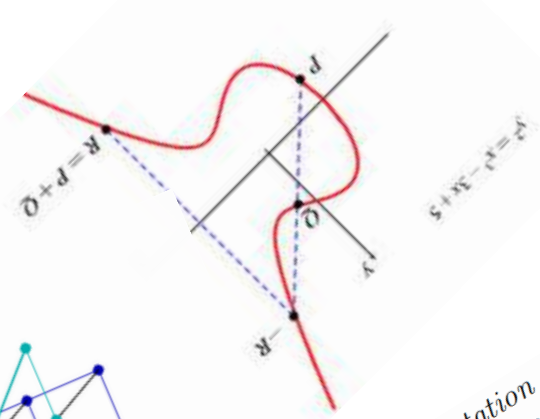
CRYPTOGRAPHY AND CRYPTANALYSIS

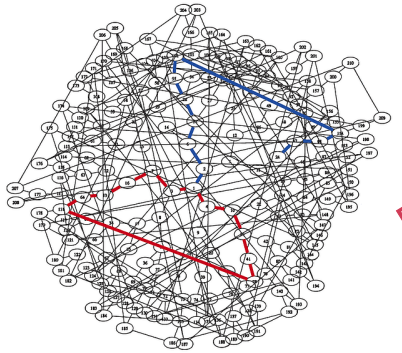
Liljana Babinkostova
Department of Mathematics

Differential Cryptanalysis



$$f(x|\mu,\sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$





Black-Box Cryptanalysis

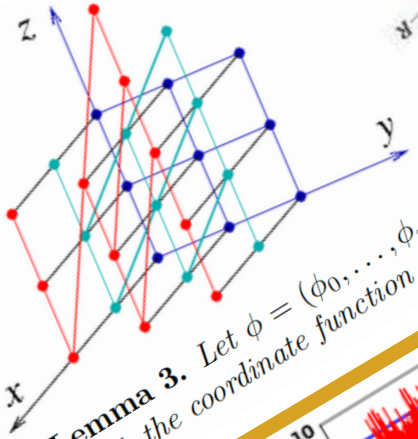
Algebraic Cryptanalysis

Side Channel Attacks

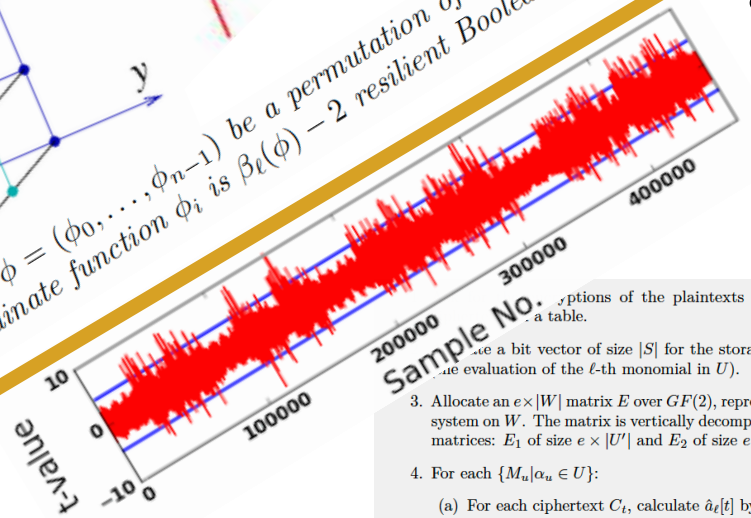
$$dp(\delta \to \Delta) \triangleq \frac{\#\{x \in \mathbb{F}_{2^n} | f(x) \oplus f(x \oplus \delta) = \Delta\}}{2^n}.$$

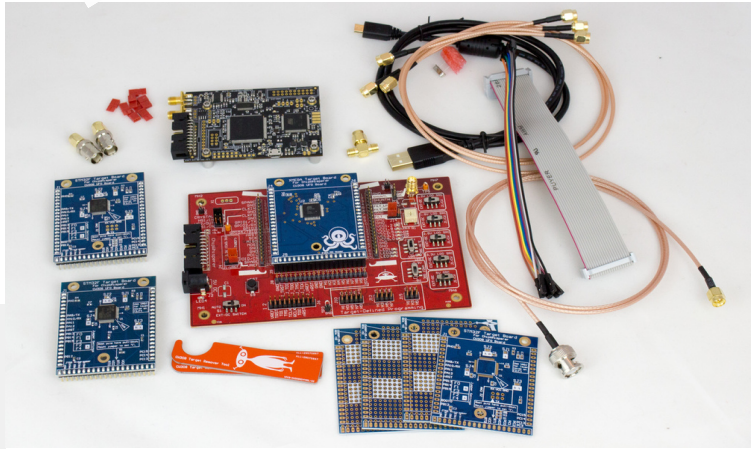
DPA

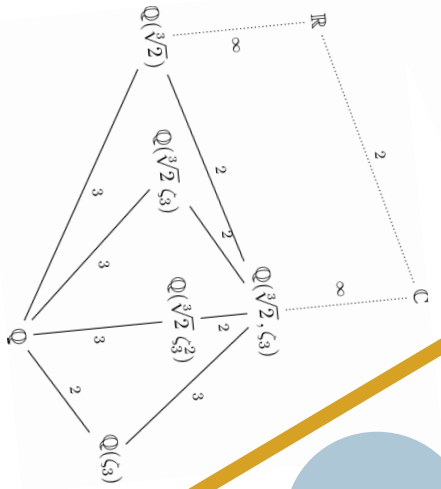
Branch Number



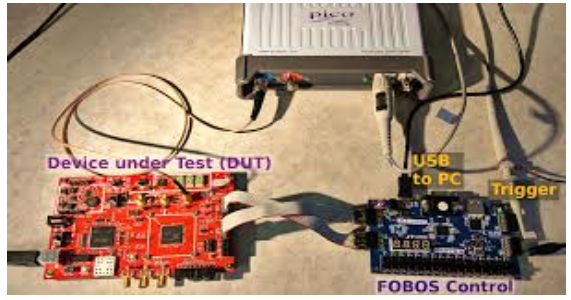
Lemma 3. *Let $\phi = (\phi_0, \ldots, \phi_{n-1})$ be a permutation of $\mathbb{F}_2^n$. For every $0 \le i \le n-1$ the coordinate function ϕ_i is $\beta_\ell(\phi) - 2$ resilient Boolean function.*



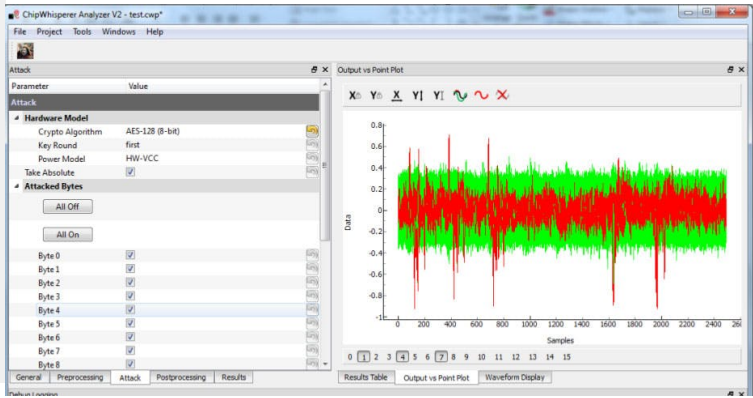




CPA



3. Allocate an $e \times |W|$ matrix E over $GF(2)$, representing the equation system on W. The matrix is vertically decomposed into two smaller matrices: E_1 of size $e \times |U'|$ and E_2 of size $e \times |V|$.
4. For each $\{M_u | \alpha_u \in U\}$:
   (a) For each ciphertext C_t, calculate $\hat{a}_\ell[t]$ by evaluating $M_u(C_t)$.
   (b) Use the Möbius transform to sum over all subspaces of $\hat{a}_\ell$.
   (c) When $\alpha_u \in U'$: For each subspace S_j in S, obtain its corresponding sum from $\hat{a}_\ell$ and copy it to the corresponding column of $E_1[j]$.
   (d) Otherwise, when $\alpha_u \in U''$: Interpolate the coefficients β_v of $V_{\le(d-i)}$ in α_u. For each subspace S_j in S, obtain its corresponding Boolean sum from $\hat{a}_l$ as the coefficient of α_u over U. Populate the corresponding column of $E_2[j]$ by adding the sum when β_v is 1.
5. Solve the equation system $E\hat{x} = \hat{a}_0$, where $\hat{x}$ represents the vector of variables of $W = U' \bigcup V$.
6. Deduce the κ-bit secret key, which is simply given by the monomials V_1.

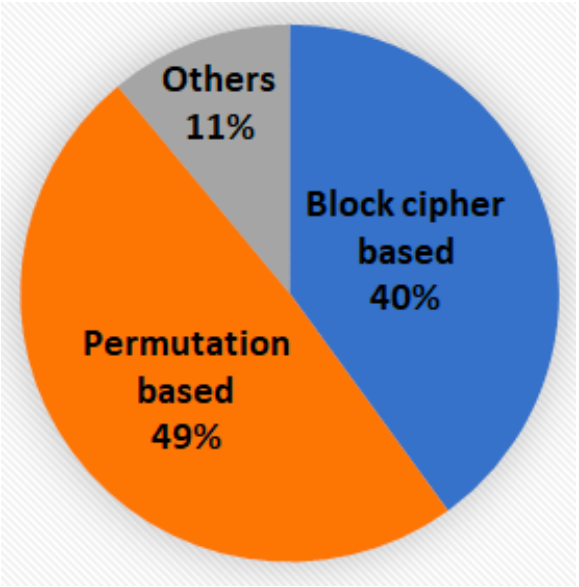


LIGHTWEIGHT AND POST-QUANTUM CRYPTOGRAPHY

National Institute of Standard and Technology

GOAL. Developing new guidelines, recommendations and standards for constrained environments when the performance of the current NIST standards is not acceptable.

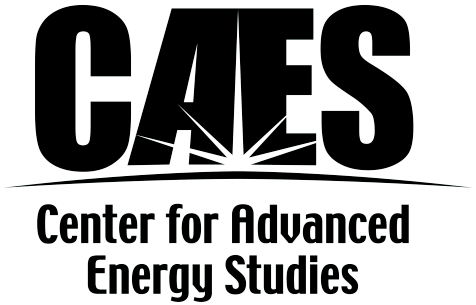
SCOPE. Symmetric-key cryptography, Authenticated Encryption with Associated Data (AEAD) Post-Quantum cryptography.



"Welcome to the next two decades ....."
- D. Apon (NIST)

- Side channel resistance? Hardware issues?
- Algebraic cryptanalysis of cyclotomics

Acknowledgment



QUESTIONS?