# Symmetric Cryptanalytic Techniques

**Sean Murphy**

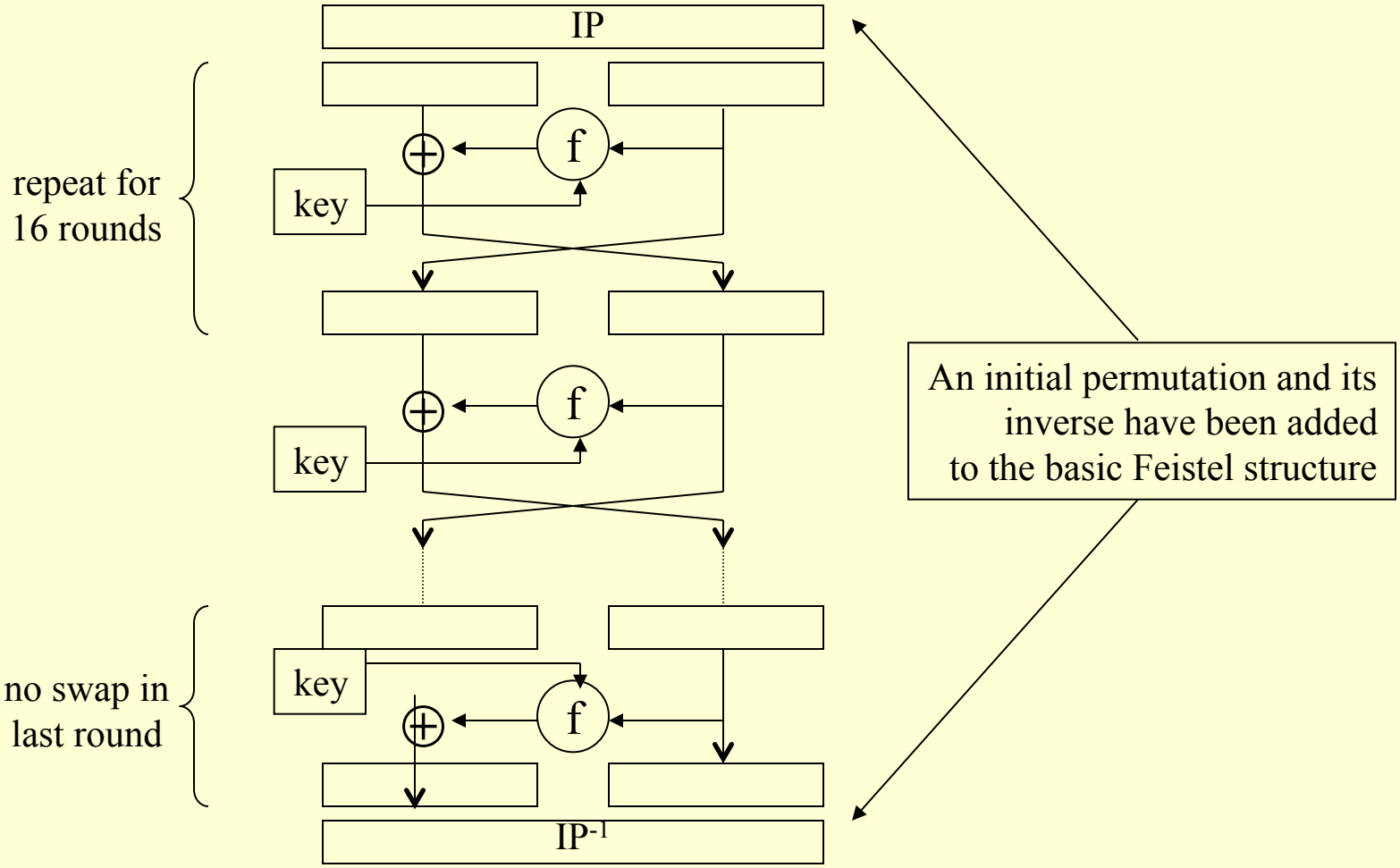
**ショーン・マーフィー**

**Royal Holloway**

# Block Ciphers

- Encrypt blocks of data using a key
  - Iterative process (“rounds”)
  - Modified by “Modes of Operation”
- Data Encryption Standard (DES) 1977
  - 64-bit blocks, 56-bit key and 16 rounds
- Advanced Encryption Standard (AES) 2000
  - 128-bit blocks, 128-bit key and 10 rounds

# Data Encryption Standard



# Generic Block Cipher Cryptanalytic Techniques

- Differential Cryptanalysis
  - Pairs of plaintexts with known relationship
  - Chosen ciphertext analysis
  - DES: Biham & Shamir 1992
- Linear Cryptanalysis
  - Random plaintext
  - Known plaintext analysis
  - DES: Matsui 1993

# Differential Cryptanalysis I

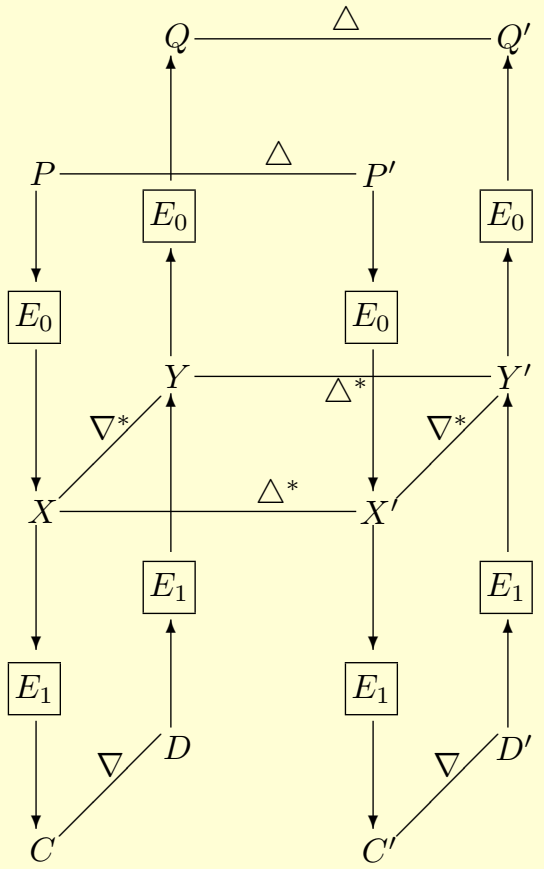
- Block Cipher Round $i$: $X$ mapped to $f(X+k_i)$
- Round $i$ Input Pair: $X_i$ and $X_i+\Delta_i$
  - Round $i$ Input difference is $X_i+(X_i+\Delta_i) = \Delta_i$
  - Input difference to $f$ is $(X_i+k_i)+(X_i+\Delta_i+k_i) =\Delta_i$
  - Input difference to $f$ does not depend on $k_i$
- Round $i$ Output Pair: $f(X_i+k_i)$ and $f(X_i+\Delta_i+k_i)$
  - Output difference is $f(X_i+k_i)+f(X_i+\Delta_i+k_i)$

# Differential Cryptanalysis II

- Round $i$
  - Difference $\Delta_i$ becomes Difference $\Delta_{i+1}$
  - Probability $p_i$
- Overall after $R$ rounds
  - Initial Difference $\Delta_0$ becomes Difference $\Delta_R$
  - Overall Probability $p_1 \ldots p_R$
- Key can be recovered for large $p_1 \ldots p_R$
  - DES: $\Delta_i$=19600000 with $p_{2i}$=1/234.

# “Boomerang Effect” (1999)

- $\Delta \rightarrow \Delta^*$ under $E_0$ prob. $p_0$
- $\nabla \rightarrow \nabla^*$ under $E_1^{-1}$ prob. $p_1$
- Choose $P$ and $P`$
  - Encrypt to $C$ and $C`$
  - Choose $D$ and $D`$
  - Decrypt to $Q$ and $Q`$
- Claim: $Q + Q` = \Delta$ prob. $p_0^2 p_1^2$



# Boomerang Analysis

- 4-Round DES
  - $E_0$ and $E_1$ are 2 rounds of DES
- $\Delta=\Delta^*=19600000$ and $\nabla=\nabla^*=1B600000$
  - Probabilities $p_0=p_1=1/234$
- Probability of Boomerang Effect is 0
- Claim based on conditional probability
  - Assertion that Conditioning Event has rank $2n$
  - Actual Conditioning Event has rank $3n$

# Linear Cryptanalysis I

- Block Cipher Round $i$: $X$ mapped to $f(X+k_i)$
- Round $i$ Input: $X_i$
  - Round $i$ Input projection by $a_i$ is $a_i^{\mathrm{T}}X_i$
  - Input projection to $f$ is $a_i^{\mathrm{T}}(X+k_i)=a_i^{\mathrm{T}}X_i+a_i^{\mathrm{T}}k_i$
  - Input difference to $f$ does depends on $a_i^{\mathrm{T}}k_i$
- Round $i$ Output: $f(X_i+k_i)$
  - Round $i$ Output projection is $a^{\mathrm{T}}_{i+1}f(X_i+k_i)$

# Linear Cryptanalysis II

- Round $i$
  - $a_i^{\mathrm{T}} X_i + a^{\mathrm{T}}_{i+1} f(X_i + k_i) = a_i^{\mathrm{T}} k_i$ probability $\frac{1}{2}(1+\varepsilon_i)$
  - $\varepsilon_i$ is the *imbalance* and $2\varepsilon_i$ is the *bias*
- Overall after $R$ rounds
  - $a_0^{\mathrm{T}} X_0 + a^{\mathrm{T}}_R X_R = c^{\mathrm{T}} K$
  - Overall Probability $\frac{1}{2}(1+\varepsilon_{0 \ldots} \varepsilon_{R-1})$
- Key can be recovered for large $|\varepsilon_{0 \ldots} \varepsilon_{R-1}|$
  - DES: Chain of $a_0 \ldots a_R$ with $|\varepsilon_{0 \ldots} \varepsilon_{R-1}| \approx 2^{-24}$

# The Linear Hull Effect

- A specific linear approximation, can be explained by multiple linear approximations each involving a different set of key bits. Such a set of linear characteristics with identical input and output masks is called a *linear hull*.
- If the set of keys used in different linear characteristics are independent, then this effect might considerably re- duce the average bias of [a single linear] expression.
- Nyberg's paper [1994] shows that attacks … will typically benefit from a linear hull effect.

*Encyclopedia of Cryptography and Security*

# Linear Hull Terminology

- Pot($a,b;k$) = | $\mathbf{P}(a^{\mathrm{T}}X+b^{\mathrm{T}}\mathrm{E}(X,k)=0)$-½ |$^2$
  - Potential of $a^{\mathrm{T}}X+b^{\mathrm{T}}\mathrm{E}(X,k)$ for key $k$
- Pot($a,b,c$) = | $\mathbf{P}(a^{\mathrm{T}}X+b^{\mathrm{T}}\mathrm{E}(X,K)+c^{\mathrm{T}}K=0)$-½ |$^2$
  - Potential of $a^{\mathrm{T}}X+b^{\mathrm{T}}\mathrm{E}(X,K)+c^{\mathrm{T}}K$
  - Approximate Linear Hull $ALH(a,b)$
- "Fundamental Theorem"
  - Average Potential of $a^{\mathrm{T}}X+b^{\mathrm{T}}\mathrm{E}(X,k)$ over the keys $k$ is the potential of the corresponding Approximate Linear Hull $ALH(a,b)$

# Simultaneous Approximations

- Independent Linear Approximations
  - $a^{\mathrm{T}}X+b^{\mathrm{T}}\mathrm{E}(X,K) = c^{\mathrm{T}}K$ probability $\frac{1}{2}(1+\varepsilon)$
  - $a^{\mathrm{T}}X+b^{\mathrm{T}}\mathrm{E}(X,K) = \gamma^{\mathrm{T}}K$ probability $\frac{1}{2}(1+\delta)$
- Addition of Approximations
  - $0 = (c+\gamma)^{\mathrm{T}}\mathrm{K}$ probability $\frac{1}{2}(1+\varepsilon\delta)$
  - Information about one key bit with **no** data
- Such linear approximations cannot be statistically independent

# Fundamental Probability

- $q(k)=\mathbf{P}_k(a^{\mathrm{T}}X+b^{\mathrm{T}}E(X,k)=0)$
- Fundamental Theorem asserts equality of
  - $\mathbf{E}\,[\,((q(k)-½)^2)^{-1}\,]$
  - $\mathbf{E}\,[\,(q(k)-½)^2\,]^{-1}$
- Jensen's Inequality for convex funtion $\Psi$
  - $\Psi(\mathbf{E}(Z)) \leq \mathbf{E}(\Psi(Z))$
  - Inversion of positive numbers is convex

# A "Linear Hull" Example

- Fundamental Probability
  - $q(k)=\mathbf{P}_k(a^{\mathrm{T}}X+b^{\mathrm{T}}E(X,k)=0)$
    $=½(1+(-1)^{c.k}\,\varepsilon+(-1)^{\gamma.k}\,\varepsilon)$
- Alternative Expression
  - $q(k)=½(1+2\varepsilon)$ if $c^{\mathrm{T}}k=\gamma^{\mathrm{T}}k=0$
  - $q(k)=½(1-2\varepsilon)$ if $c^{\mathrm{T}}k=\gamma^{\mathrm{T}}k=1$
  - $q(k)=½$ if $c^{\mathrm{T}}k\neq\gamma^{\mathrm{T}}k$
- Linear Hull asserts possible to find $c^{\mathrm{T}}k$ **and** $\gamma^{\mathrm{T}}k$

# Cryptographic Conclusions

- Probabilistic assumptions matter
- Probabilistic reasoning matters
- Fundamental errors in simple situations