CS641

Modern Cryptology

Lecture 10

Square Attack: Setup

- Classify a given set of 256 byte values into four categories:
  - P: all 256 values are distinct
  - C: all 256 values are identical
  - Z: XOR of all 256 values equals zero
  - X: all patterns
- Clearly, P and C are also Z, and all three are also X.
- We aim classification into most restrictive pattern.

Square Attack: Setup

- Given a set of 256 plaintext blocks, we can write pattern category for each of the 16 bytes in it.
- We represent this also as a matrix.
- For example, 256 plaintext blocks that differ only in the first byte represent pattern:

$$\begin{bmatrix} P & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix}.$$

- And 256 plaintext blocks that are all 0's, all 1's, ..., all 255's represent pattern:

$$\begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix}.$$

Square Attack: Analysis

- Let us analyze the effect of each of AES operations on different patterns.
- All operations except MixColumn operate on bytes, and MixColumn operates on columns.
- Therefore, except MixColumn, other operations effect byte pattern.
- MixColumn effects column pattern.

Square Attack: Analysis of ByteSub

- ByteSub operation has following effect on various patterns:
  - P goes to P.
  - C goes to C.
  - Z goes to X.
  - X goes to X.

Square Attack: Analysis of ShiftRow

- ShiftRow operation has following effect on various patterns:
  - P goes to P.
  - C goes to C.
  - Z goes to Z.
  - X goes to X.

Square Attack: Analysis of AddRoundKey

- AddRoundKey operation has following effect on various patterns:
  - P goes to P.
  - C goes to C.
  - Z goes to Z.
  - X goes to X.

Square Attack: Analysis of MixColumn

- MixColumn operation has following effect on various patterns:

$$\begin{bmatrix} C \\ C \\ C \\ C \end{bmatrix} \Rightarrow \begin{bmatrix} C \\ C \\ C \\ C \end{bmatrix}$$

$$\begin{bmatrix} P \\ C \\ C \\ C \end{bmatrix} \Rightarrow \begin{bmatrix} P \\ P \\ P \\ P \end{bmatrix}$$

$$\begin{bmatrix} P \\ P \\ C \\ C \end{bmatrix} \Rightarrow \begin{bmatrix} Z \\ Z \\ Z \\ Z \end{bmatrix}$$

Square Attack: Analysis of MixColumn

- $\begin{bmatrix} P \\ P \\ P \\ P \end{bmatrix} \Rightarrow \begin{bmatrix} Z \\ Z \\ Z \\ Z \end{bmatrix}$:
  - Let $v_1, \ldots, v_{256}$ be input vectors with $v_i = \begin{bmatrix} \alpha_{i1} \\ \alpha_{i2} \\ \alpha_{i3} \\ \alpha_{i4} \end{bmatrix}$.
  - Let $u_i = M \cdot v_i = \begin{bmatrix} \beta_{i1} \\ \beta_{i2} \\ \beta i3 \\ \beta i4 \end{bmatrix}$.
  - We have $\beta_{i,j} = \sum_{k=1}^{4} M[j,k]\alpha_{i,k}$.
  - Therefore,

$$\sum_{i=1}^{256} \beta_{i,j} = \sum_{k=1}^{k} M[j,k] \sum_{i=1}^{256} \alpha_{i,k} = 0.$$

Square Attack: Three Rounds of AES

- Input pattern:

$$\begin{bmatrix} P & C & C & C \\ P & C & C & C \\ P & C & C & C \\ P & C & C & C \end{bmatrix}.$$

- Pattern movement (before first round):

$$\begin{bmatrix} P & C & C & C \\ P & C & C & C \\ P & C & C & C \\ P & C & C & C \end{bmatrix} \xrightarrow[\Rightarrow]{\text{AddRoundKey}} \begin{bmatrix} P & C & C & C \\ P & C & C & C \\ P & C & C & C \\ P & C & C & C \end{bmatrix}$$

Square Attack: Three Rounds of AES

- Pattern movement (first round):

$$\begin{bmatrix} P & C & C & C \\ P & C & C & C \\ P & C & C & C \\ P & C & C & C \end{bmatrix} \xrightarrow{\text{ByteSub}} \begin{bmatrix} P & C & C & C \\ P & C & C & C \\ P & C & C & C \\ P & C & C & C \end{bmatrix}$$

$$\begin{bmatrix} P & C & C & C \\ P & C & C & C \\ P & C & C & C \\ P & C & C & C \end{bmatrix} \xrightarrow{\text{ShiftRow}} \begin{bmatrix} P & C & C & C \\ C & C & C & P \\ C & C & P & C \\ C & P & C & C \end{bmatrix}$$

Square Attack: Three Rounds of AES

- Pattern movement (first round):

$$\begin{bmatrix} P & C & C & C \\ C & C & C & P \\ C & C & P & C \\ C & P & C & C \end{bmatrix} \xrightarrow{\text{MixColumn}} \begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix}$$

$$\begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix} \xrightarrow{\text{AddRoundKey}} \begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix}$$

Square Attack: Three Rounds of AES

- Pattern movement (second round):

$$\begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix} \xrightarrow{\text{ByteSub}} \begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix}$$

$$\begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix} \xrightarrow{\text{ShiftRow}} \begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix}$$

Square Attack: Three Rounds of AES

- Pattern movement (second round):

$$\begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix} \xrightarrow{\text{MixColumn}} \begin{bmatrix} Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{bmatrix}$$

$$\begin{bmatrix} Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{bmatrix} \xrightarrow{\text{AddRoundKey}} \begin{bmatrix} Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{bmatrix}$$

Square Attack: Three Rounds of AES

- Pattern movement (third round):

$$\begin{bmatrix} Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{bmatrix} \xrightarrow[\Rightarrow]{\text{ByteSub+AddRoundKey}} \begin{bmatrix} X & X & X & X \\ X & X & X & X \\ X & X & X & X \\ X & X & X & X \end{bmatrix}$$

- ShiftRow of last round can be undone.

Square Attack: Three Rounds of AES

- Let $[\beta_{i,j,k}]$ be the output ciphertext block corresponding to ith plaintext block.
- Let $[k_{3,j,k}]$ be key matrix used in third round.
- For every $0 \leq j, k \leq 3$, do the following:
  - Guess value of $k_{3,j,k}$.
  - Decrypt $\beta_{i,j,k}$ for one round to compute 256 values.
  - Check if they sum to zero.
  - If not, the guess for $k_{3,j,k}$ was wrong and can be discarded.

Square Attack: Three Rounds of AES

- In this way, wrong values of $k_{3,j,k}$ can be eliminated.
- It will require a few sets of 256 plaintext block with the specified pattern.
- This allows last round key to be recovered very efficiently.
- From this, the keys of all rounds can be computed.

Square Attack: Four Rounds of AES

- Input pattern:

$$\begin{bmatrix} P & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix}.$$

- Pattern movement (before first round):

$$\begin{bmatrix} P & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix} \xrightarrow[\Rightarrow]{\text{AddRoundKey}} \begin{bmatrix} P & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix}$$

Square Attack: Four Rounds of AES

- Pattern movement (first round):

$$\begin{bmatrix} P & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix} \xrightarrow{\text{ByteSub}} \begin{bmatrix} P & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix}$$

$$\begin{bmatrix} P & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix} \xrightarrow{\text{ShiftRow}} \begin{bmatrix} P & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix}$$

Square Attack: Four Rounds of AES

- Pattern movement (first round):

$$\begin{bmatrix} P & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix} \xrightarrow{\text{MixColumn}} \begin{bmatrix} P & C & C & C \\ P & C & C & C \\ P & C & C & C \\ P & C & C & C \end{bmatrix}$$

$$\begin{bmatrix} P & C & C & C \\ P & C & C & C \\ P & C & C & C \\ P & C & C & C \end{bmatrix} \xrightarrow{\text{AddRoundKey}} \begin{bmatrix} P & C & C & C \\ P & C & C & C \\ P & C & C & C \\ P & C & C & C \end{bmatrix}$$

Square Attack: Four Rounds of AES

- Pattern movement (second round):

$$\begin{bmatrix} P & C & C & C \\ P & C & C & C \\ P & C & C & C \\ P & C & C & C \end{bmatrix} \xrightarrow{\text{ByteSub}} \begin{bmatrix} P & C & C & C \\ P & C & C & C \\ P & C & C & C \\ P & C & C & C \end{bmatrix}$$

$$\begin{bmatrix} P & C & C & C \\ P & C & C & C \\ P & C & C & C \\ P & C & C & C \end{bmatrix} \xrightarrow{\text{ShiftRow}} \begin{bmatrix} P & C & C & C \\ C & C & C & P \\ C & C & P & C \\ C & P & C & C \end{bmatrix}$$

Square Attack: Four Rounds of AES

- Pattern movement (second round):

$$\begin{bmatrix} P & C & C & C \\ C & C & C & P \\ C & C & P & C \\ C & P & C & C \end{bmatrix} \xRightarrow{\text{MixColumn}} \begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix}$$

$$\begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix} \xRightarrow{\text{AddRoundKey}} \begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix}$$

Square Attack: Four Rounds of AES

- Pattern movement (third round):

$$\begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix} \xrightarrow{\text{ByteSub}} \begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix}$$

$$\begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix} \xrightarrow{\text{ShiftRow}} \begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix}$$

Square Attack: Four Rounds of AES

- Pattern movement (third round):

$$\begin{bmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{bmatrix} \xrightarrow{\text{MixColumn}} \begin{bmatrix} Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{bmatrix}$$

$$\begin{bmatrix} Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{bmatrix} \xrightarrow{\text{AddRoundKey}} \begin{bmatrix} Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{bmatrix}$$

Square Attack: Four Rounds of AES

- Pattern movement (fourth round):

$$\begin{bmatrix} Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{bmatrix} \xrightarrow[\Rightarrow]{\text{ByteSub+AddRoundKey}} \begin{bmatrix} X & X & X & X \\ X & X & X & X \\ X & X & X & X \\ X & X & X & X \end{bmatrix}$$

- ShiftRow of last round can be undone.
- This can be broken in exactly same way as three round AES.

Current Status of AES Attacks

- AES can be efficiently broken only up to four rounds.
- There exists a chosen-ciphertext attack on full 10-round AES that takes time slightly less than brute-force: $\approx 2^{126}$ steps.