Optimizing Diffusion and Confusion in Cryptographic Primitives

Christopher A. Wood

May 9, 2012

Agenda

1. Cryptographic algorithm security fundamentals
2. Design Criteria
3. Case study: Rijndael
4. Open problems and future work

Algorithm security fundamentals

- Strive for high confusion and diffusion
  - *Confusion* - complex relationship between the secret key and ciphertext
  - *Diffusion* - dissipation of plaintext bits throughout ciphertext bits

Algorithm construction principles

- Algorithms are composed of a combination of linear and nonlinear operations
- Maximize diffusion through linear transformations
  - Linear permutations
  - Circular shifts
  - Modular addition
- Maximize confusion through nonlinear operations
  - S(ubstitution)-box (Rijndael cipher)
  - Add-Rotate-XOR (ARX) combination functions (Threefish cipher)
  - Discrete-time difference equations (often defined as recurrence relations)

Measuring security

- Linear behavior
  - Exhibit avalanche effect and adherence to Strict Avalanche Criterion (SAC)
- Nonlinear behavior
  - Branch number
  - Direct measurement of nonlinear behavior

Avalanche effect

A function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ exhibits the *avalanche effect* if and only if

$$\sum_{x \in \mathbb{F}_2^n} \text{wt}(f(x) \oplus f(x \oplus c_i^n)) = n2^{n-1}, *$$

for all $i(1 \leq i \leq n)$, where $c_i^n = [0, 0, \ldots, 1, \ldots, 0]$ (where a 1 is in the nth position of the vector of cardinality n).

*wt indicates the Hamming Weight function

SAC

A function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ satisfies the *Strict Avalanche Critertion (SAC)* if for all $i(1 \leq i \leq n)$ the following equations hold:

$$\sum_{x \in \mathbb{F}_2^n} f(x) \oplus f(x \oplus c_i^n) = (2^{n-1}, 2^{n-1}, ..., 2^{n-1})$$

This simply means that $f(x) \oplus f(x \oplus c_i^n)$ is balanced for every element in $\mathbb{F}_2^n$ with Hamming distance of 1.

Branch number

The *branch number* of an $n \times n$-bit S-Box is

$$BN = \min_{a,b \neq a}(\text{wt}(a \oplus b) + \text{wt}(S(a) \oplus S(b))),$$

where $a, b \in \mathbb{F}_2^n$.

S-box specific nonlinear measurements

The nonlinearity of an $n \times n$-bit S-Box from $\mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ can be measured by

$$P_S = \max_{0 \neq a,b} |\{x \in \mathbb{F}_2^n : S(x+a) - S(x) = b\}|$$

where $a, b \in \mathbb{F}_2^n$.

Implementation Considerations

- Design against common cryptanalysis techniques
- Linear transformations
  - Linear permutations
  - Circular shifts
  - Modular addition
- Nonlinear transformations
  - S-boxes
  - ARX functions
  - Chaotic recurrence relations

S-boxes

- Bijective functions from $\mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$.
- Designed for optimal nonlinearity and algebraic complexity.
  - Maximize the avalanche property of the S-box for all input/output pairs.
  - Minimize the differential propagation probability
  - Maximize complexity of the algebraic expression for the S-box in $\mathbb{F}_2^n$

Rijndael Substitute Bytes Calculation

Rijndael sub-bytes affine transformation

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Rijndael Substitute Bytes Calculation

This affine can also be represented algebraically as follows

$$b'_i = b_i \oplus b_{(i+4)mod8} \oplus b_{(i+5)mod8} \oplus b_{(i+6)mod8} \oplus b_{(i+7)mod8} \oplus c_i$$

where i is the ith bit of the input byte b and $c = \langle 01100011 \rangle$.

S-boxes

- Random and fixed structure (i.e. Rijndael s-box) designs have been propsed based on susceptibility to differential cryptanalysis
  - Fixed structure are more beneficial for security analysis and proof purposes
- Various construction criterias have been proposed
  - Nydberg (91) - *"A perfect nonlinear S-box is a substitution transformation with evenly distributed directional derivatives."*
  - Dawson and Tavares (91) - static and dynamic criteria supporting claim for high branch numbers and avalanche property
  - ...

Provable Security for S-boxes

Theorem: (KN Theorem) It is assumed that in a DES-like cipher with $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$ (the substitution function) the keys are independent and uniformly random. Then, the probability of an s-round differential, $s \geq 4$, is less than or equal to p_{max}^2, where p_{max} is defined in terms of the nonlinearity of the S-box as follows:

$$p_{max} \leq max_b max_{a \neq 0} Pr[f(Y + a) + f(a) = b],$$

where $a, b \in \mathbb{F}_2^n$.

Similar Nonlinear Functions

- Bent functions
- Vector bent functions
- APN S-boxes
- Differentially Uniform δ-Uniform S-box functions
- ...

Bent Functions

The correlation between a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and a linear function $x \mapsto u \cdot x$ is defined as

$$c_f(u) = \frac{1}{2^n}(|\{x \in \mathbb{F}_2^n : f(x) = u \cdot x\} - |\{x \in \mathbb{F}_2^n : f(x) \neq u \cdot x\})$$

A Boolean function is thus called *bent* if

$$|c_f(u)| = 2^{\frac{-n}{2}},$$

for all $u \in \mathbb{F}_2^n$. Note that n must be even in order for f to be bent.

Vector Bent Functions

- Perfect nonlinearity of Boolean functions strongly correlates to cryptographic strength
- Nydberg's "perfect nonlinear functions" - an multiple dimension Boolean functions

A vector function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is said to be *bent* if

- $w \cdot f$ is bent for all $w \neq 0$.
- f is perfect nonlinear ($f(x+\alpha) = f(x)$ is uniformly distributed as x varies, for all fixed $\alpha \in \mathbb{F}_2^n - \{0\}$.

APN S-boxes

A function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is said to be *almost perfect nonlinear* (APN) if

$$|\{x : f(x+\alpha) + f(x) = \beta\}| \leq 2,$$

for all fixed $\alpha \in \mathbb{F}_2^n - \{0\}$. Some examples include:

- $f : \mathbb{F}_2^n \to \mathbb{F}_2^n, f(x) = x^3$
- $f : \mathbb{F}_2^n \to \mathbb{F}_2^n, f(x) = x^{2k+1}$ (i.e. any odd power exponent)

Differentially δ-Uniform S-box functions

A function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is said to be *differentially δ-uniform* if

$$|\{x : f(x+\alpha) + f(x) = \beta\}| \leq \delta,$$

Small values for δ are desirable - indicates higher degree of nonlinearity.

ARX functions

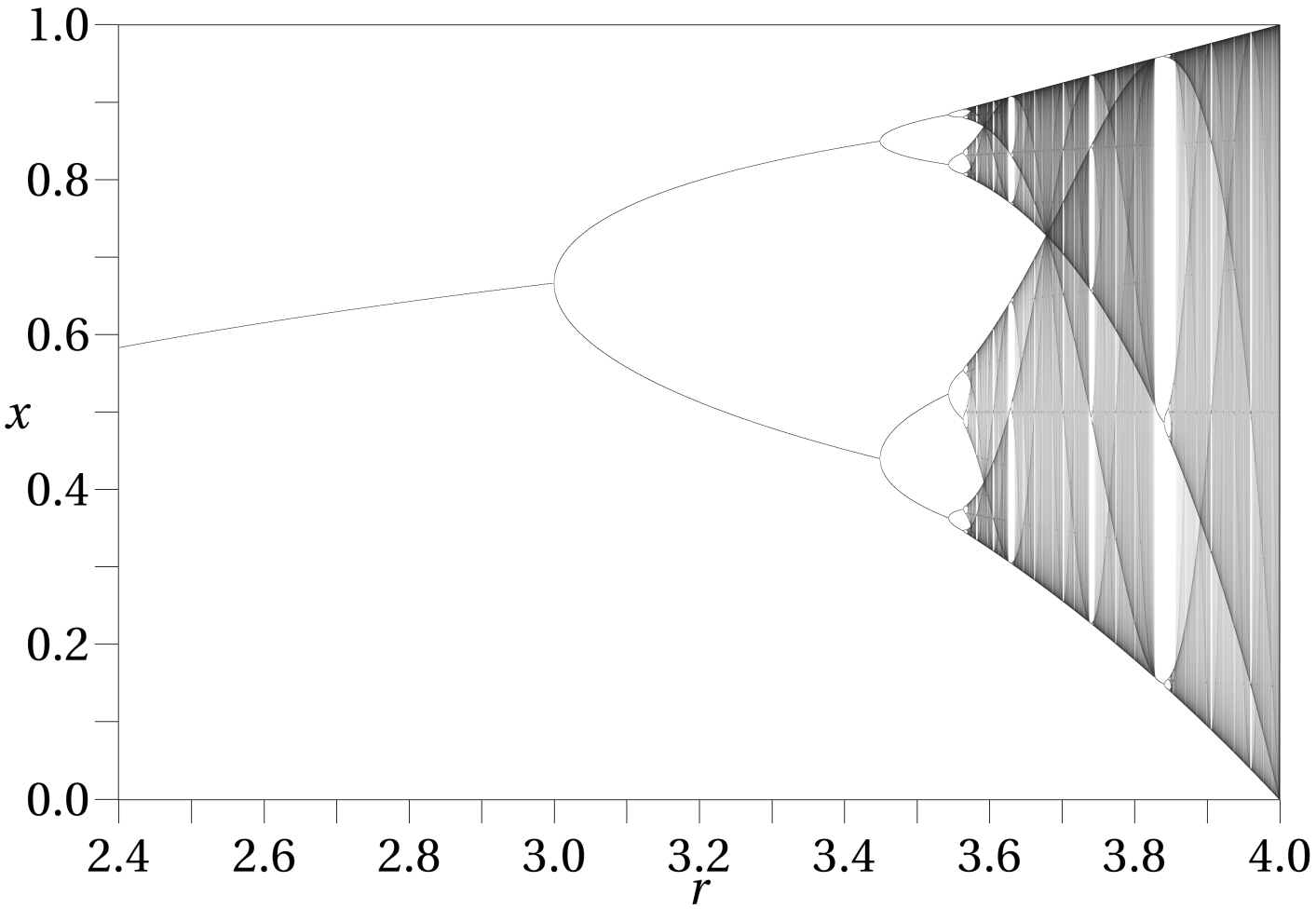
- Nonlinear functions consisting of a combination of modular addition, bitwise rotation, and bitwise XOR operations
- Analysis of differential propagation is difficult
  - Differential properties of sub-operations need to be considered ($\text{adp}^{\oplus}$, xdp^{+})
- Most susceptible to rotational cryptanalysis
  - Threefish was attacked using a combination of rotational cryptanalysis with a rebound attack (Khovratovich et al, 2010) - led to adjustment of Threefish rotation constants

Chaotic recurrence relations

- Chaotic systems are defined by:
  - Sensitivity to initial conditions
  - Topologically mixing (i.e. covers entire state space)
  - Dense (and long) periodic orbits
- Some recurrence relations exhibit "chaotic" behavior (e.g. the Logistic Map)

$$x_{n+1} = rx_n(1 - (x_n))$$

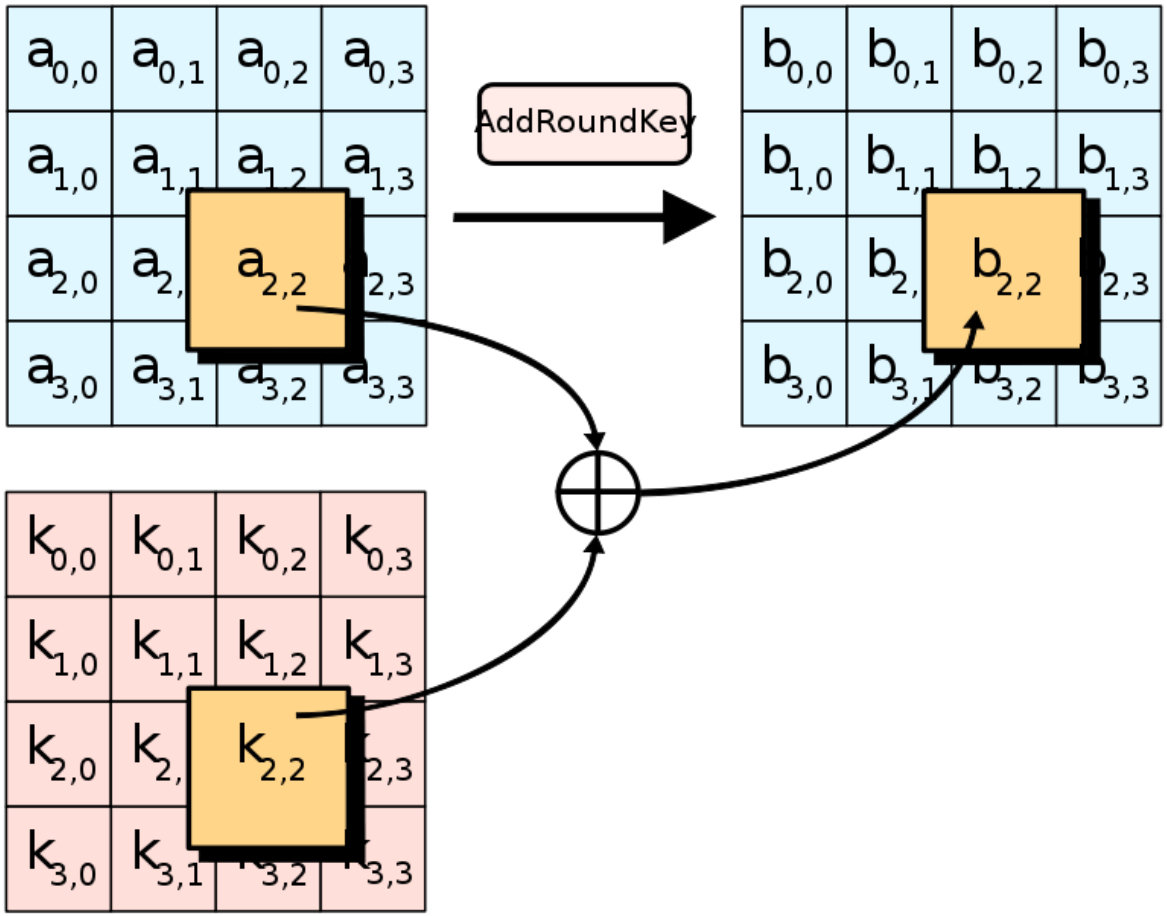
Chaos in the Logistic Map



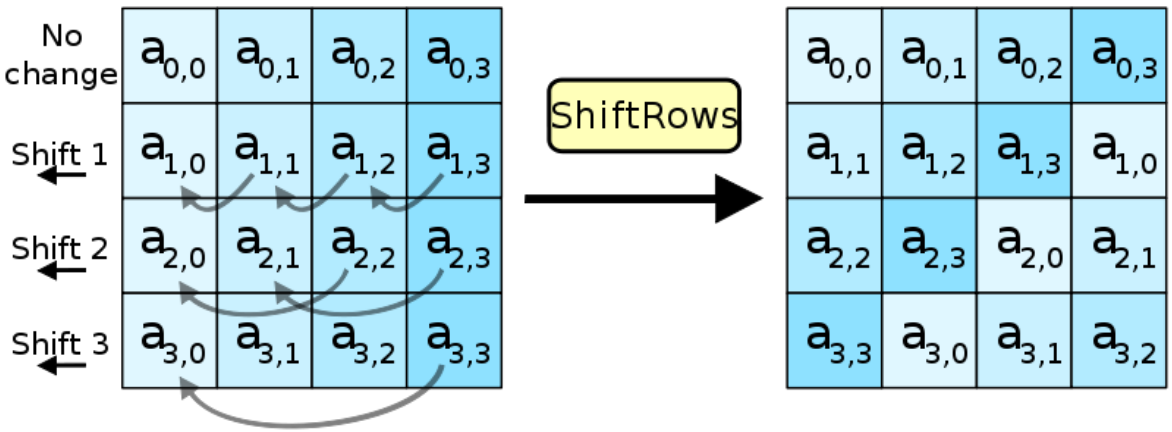
Case Study: Rijndael

- Four main operations
  - Add round key
  - Shift rows
  - Substitute bytes
  - Mix columns

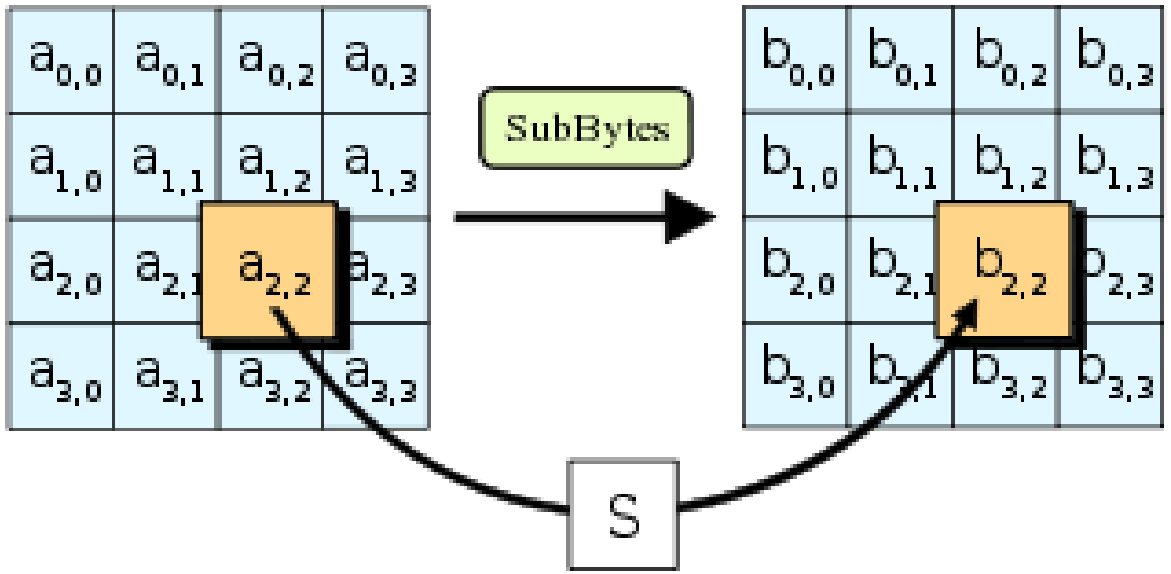
Add Round Key



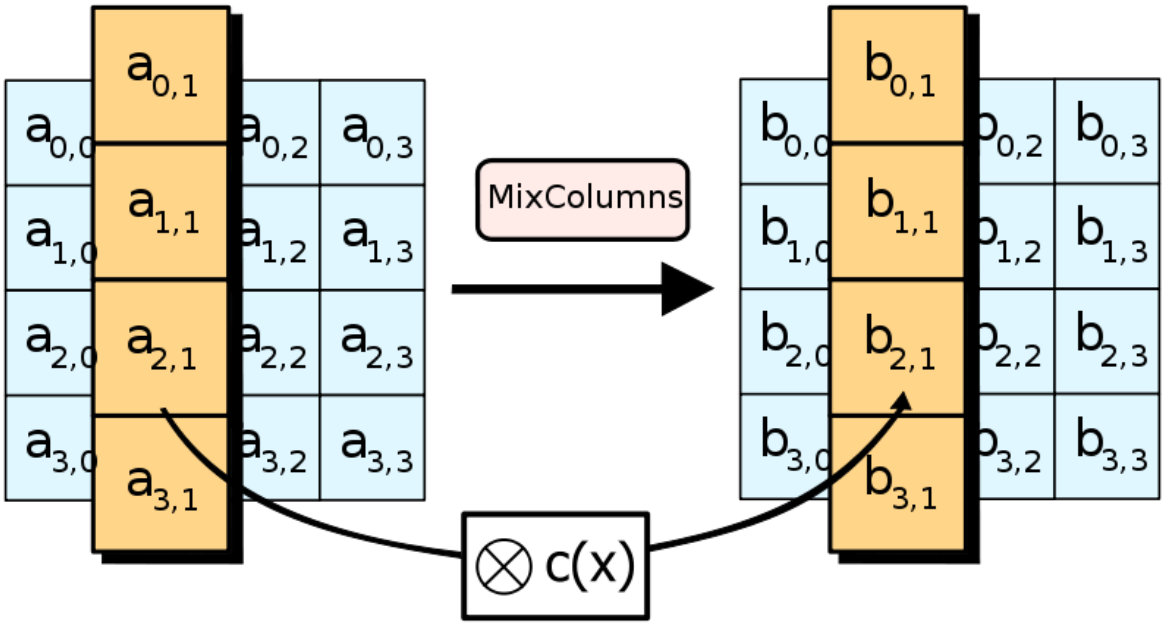
Shift Rows


No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

Substitute Bytes



Mix Columns



Mix Columns MDS Matrix

$$\begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Open problems and future work

- Diffusion and confusion are the determining factors of secure primitives
- The design space for diffusion and confusion layers is not exhausted
  - Other compositions of discrete mathematical objects and operations exist (bent functions, MDS matrices, etc)
  - Can they provide the same measure of security as existing objects (i.e. S-boxes, ARX functions)?
- How feasible is the reduction of the security of block ciphers to an multivariate optimization problem?
- How different are the implementation aspects of each of these mathematical objects?
  - Can we improve existing implementations?