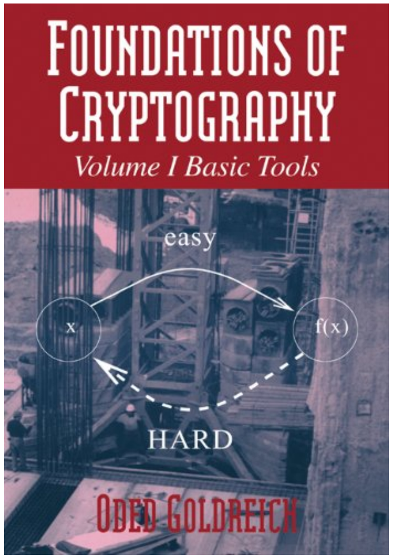
# Substitution-permutation networks, pseudorandom functions, and natural proofs

Eric Miles
Northeastern University

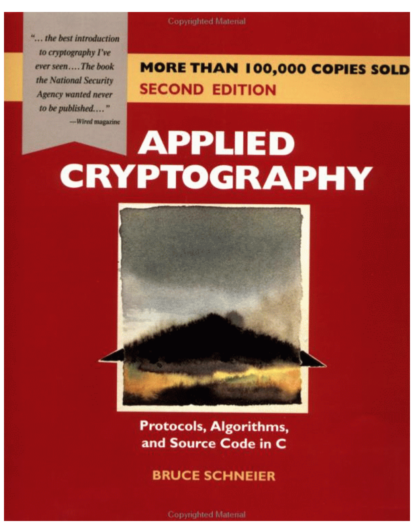
joint work with Emanuele Viola

# “Theory vs. practice” gap in cryptography




Theoreticians have . . .

- **liberal** notion of efficiency
  polynomial time
- **provable** security
  based on hardness assumptions




Practitioners have . . .

- **very efficient** algorithms
  near linear time
- **heuristic** security
  resistance to known attacks

# Common goal: random-looking functions

$\{f_K : \{0,1\}^n \rightarrow \{0,1\}^n \mid K\}$ indistinguishable from truly random function

- theory: pseudorandom function (PRF)
  [Goldreich-Goldwasser-Micali '84]

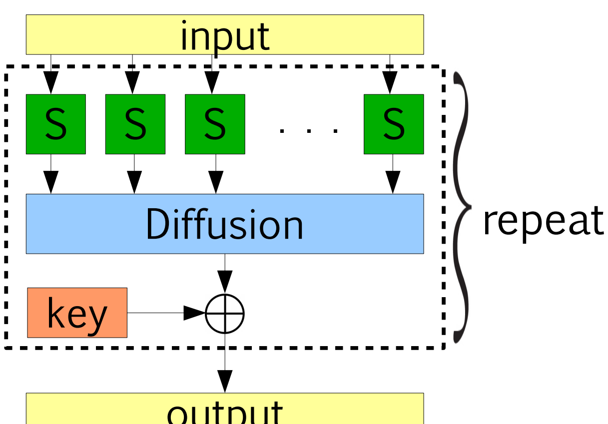
- practice: block cipher / MAC
  [Feistel '70s], [Simmons '80s]

  - NOTE: block cipher "modes" $\not\Rightarrow$ PRF

# Common goal: random-looking functions

$\{f_K : \{0,1\}^n \to \{0,1\}^n \mid K\}$ indistinguishable from truly random function

| GAPS | PRF | Block cipher / MAC |
|---|---|---|
| efficiency | best: $\lvert K \rvert \geq n^2$<br>e.g. factoring-based PRF [Naor-Reingold '04] | typical: $\lvert K \rvert \approx n$<br>e.g. Advanced Encryption Standard [Daemen-Rijmen '00] |
| methodology | - based on PRG/OWF<br>- "expensive" components<br>e.g. iterated multiplication | Substitution-permutation network |



# Our contributions: bridging the gap

**New candidate PRF based on SP-network**

- more efficient than previous candidates
- application to Natural Proofs [Razborov-Rudich '97]
- security derived from "practical" analysis

**Proof-of-concept theorem:**

**SP-network with random S-box = secure, inefficient PRF.**

- analogous to [Luby-Rackoff '88] for Feistel networks

# Outline

Introduction

**SP-network: definition and security**

New PRF candidates

SP-network with random S-box

Natural Proofs

# The SP-network paradigm

[Shannon '49, Feistel-Notz-Smith '75]

## S(ubstitution)-box

$S : GF(2^b) \longrightarrow GF(2^b)$

- computationally expensive
- good crypto properties

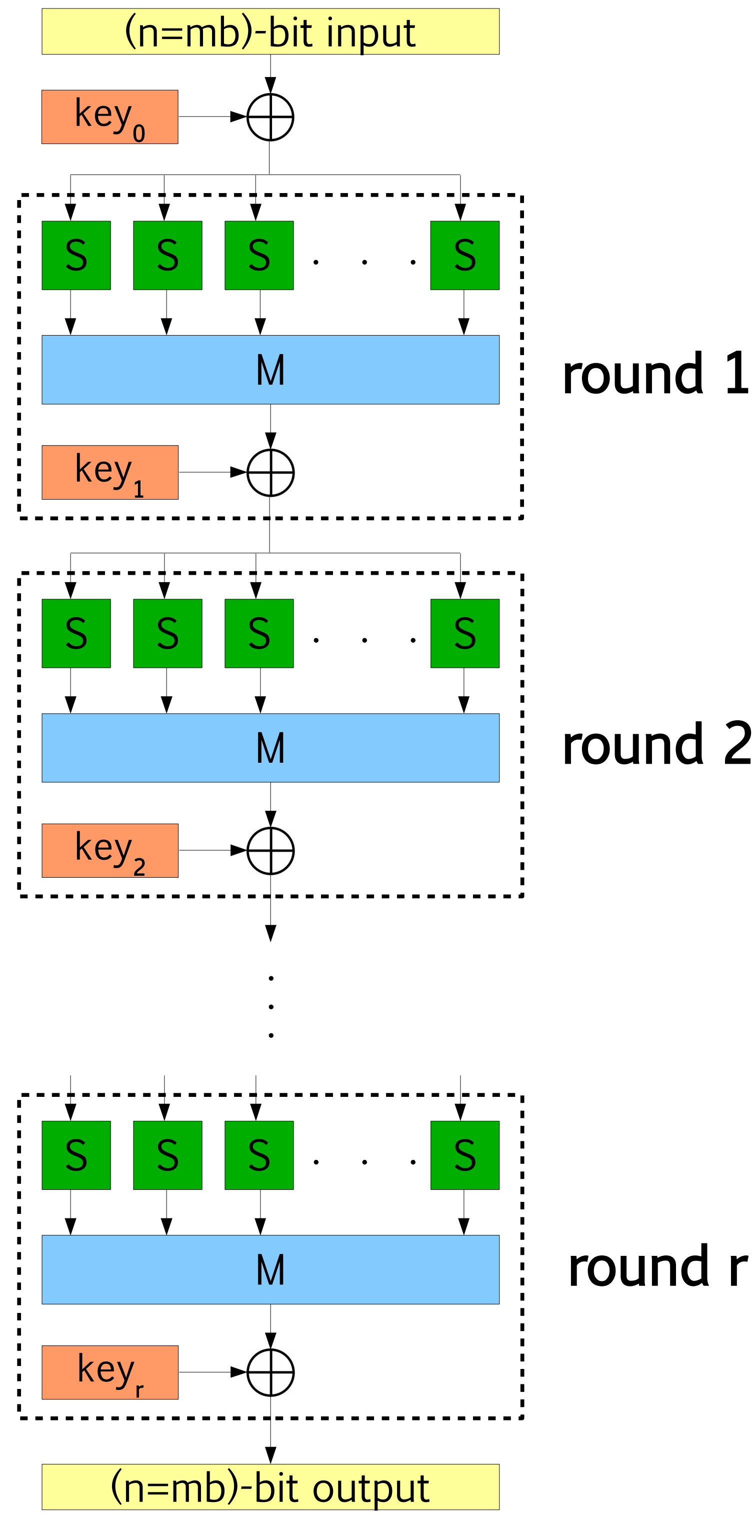
## Linear transformation

$M : GF(2^b)^m \longrightarrow GF(2^b)^m$

- computationally cheap
- good diffusion properties

## Key XOR

- only source of secrecy
- round keys = uniform, independent



# Linear and differential cryptanalysis

[Matsui '94] [Biham-Shamir '91]

Two general attacks against a block cipher **C**

- parameters of interest:

$p_{LC}(C), p_{DC}(C) \leq 2^{-\Omega(n)} \Rightarrow 2^{-\Omega(n)}$ security against LC/DC

- details:

$$p_{LC}(C) = \max_{A,B} E_K |\Pr_x [\langle A, x\rangle = \langle B, C_K(x)\rangle] - ½|^2$$

$$p_{DC}(C) = \max_{A,B} \Pr_{x,K} [C_K(x) \oplus C_K(x \oplus A) = B]$$

# LC/DC design principles

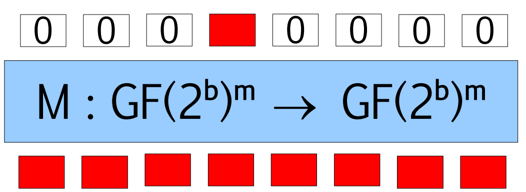
## 1. S-box resists LC/DC.

$S(x) := x^{2^b-2}$ satisfies

$p_{LC/DC}(S) \leq 2^{-(b-2)}$. [Nyberg '93]

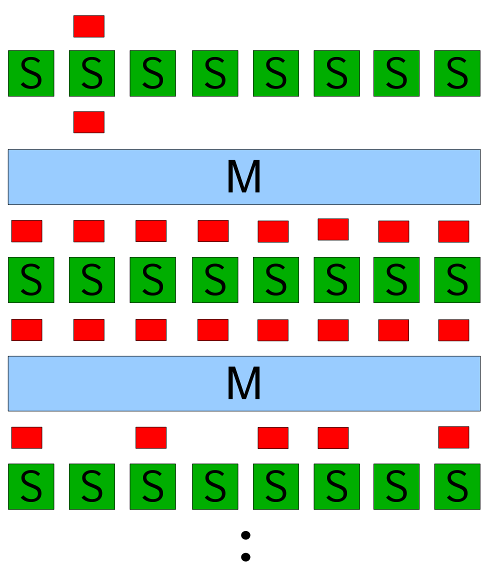
## 2. M has "branch number" Br(M) = m+1.

$$\mathrm{Br}(M) := \min_{x \neq 0^m} \{\mathrm{wgt}(x) + \mathrm{wgt}(M(x))\}$$




Intuition: 1+2 ⇒ LC/DC security

S-box security $2^{-\Omega(b)}$
propagates to m bundles
$(2^{-\Omega(b)})^m = 2^{-\Omega(n)}$



# Outline

Introduction

SP-network: definition and security

**New PRF candidates**

SP-network with random S-box

Natural Proofs

# New PRF: quasi-linear size

Theorem: $\exists$ size-$n \cdot \log^{O(1)} n$ SPN with LC/DC security $2^{-n/2}$.
[M-Viola]

Compare to best complexity PRF [Naor-Reingold '04]:

- security from factoring / discrete-log hardness
- size = $\Omega(n^2)$

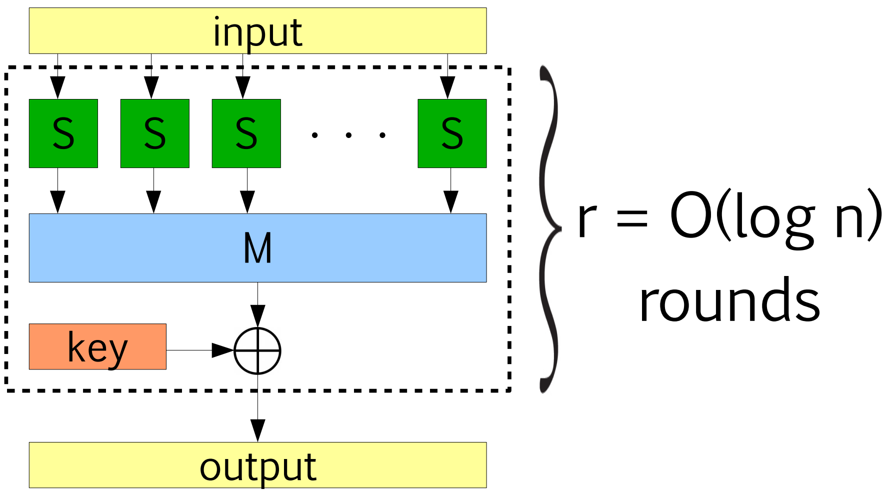
# New PRF: quasi-linear size

<u>Theorem</u>: $\exists$ size-$n \cdot \log^{O(1)} n$ SPN with LC/DC security $2^{-n/2}$.
[M-Viola]

<u>**EFFICIENCY**</u>

S-box: $\quad S(x) := x^{2^b-2}$

- $b = \log n \Rightarrow S \in$ size $\log^{O(1)} n$




## Linear transformation

- Let $G = [I \,|\, M]$ be $m \to 2m$ Reed-Solomon code.
  - this gives max branch number [Daemen '95]

- Such $M$ is a **Cauchy matrix**. [Roth-Seroussi '85]

- We adapt [Gerasoulis '88] to do Cauchy mult. in size $O(n \cdot \log^3 n)$.

# New PRF: quasi-linear size

Theorem: $\exists$ size-$n \cdot \log^{O(1)} n$ SPN with LC/DC security $2^{-n/2}$.
[M-Viola]

## SECURITY

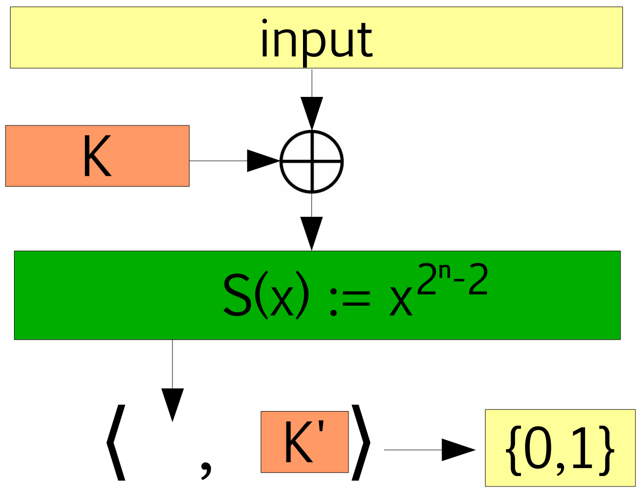
Theorem: If $p_{LC/DC}(S) \leq 2^{-(b-2)}$ and $Br(M) = m+1$,

then r-round SPN has $p_{LC/DC}(SPN) \leq 2^{-(n-rm)}$.

[Kang-Hong-Lee-Yi-Park-Lim '01, M-Viola '12]

- $r = b/2 \Rightarrow$ security $= 2^{-n/2}$ $(n = mb)$
- $S(x) = x^{2^b-2}$ has $p_{LC/DC}$ bounds [Nyberg '93]

# New PRF: simple candidate




$$C_{K,K'}(x) := \langle (x \oplus K)^{2^n-2}, K' \rangle$$

Theorem: $C_{K,K'}$ $2^{-\Omega(n)}$-fools parity tests on $\leq 2^{0.9n}$ outputs.
[M-Viola]

- compare to [Even-Mansour '91]:
  - replace EM's random f'n with S: simple attack
  - also replace $\oplus$ K' with ⟨ , K'⟩: fools parity tests
- also computable in quasi-linear size [Gao-von zur Gathen-Panario-Shoup '00]

# Outline

Introduction

SP-network: definition and security

New PRF candidates

**SP-network with random S-box**

Natural Proofs

# SP-network with random S-box

Theorem: If SP-network has: 1. random S-box
[M-Viola]
2. max-branch-number M,

then: q-query distinguishing advantage $\leq (rmq)^3 \cdot 2^{-b}$.

- when $b = \omega(\log n)$, security $= n^{-\omega(1)}$

- similar bound as Luby-Rackoff

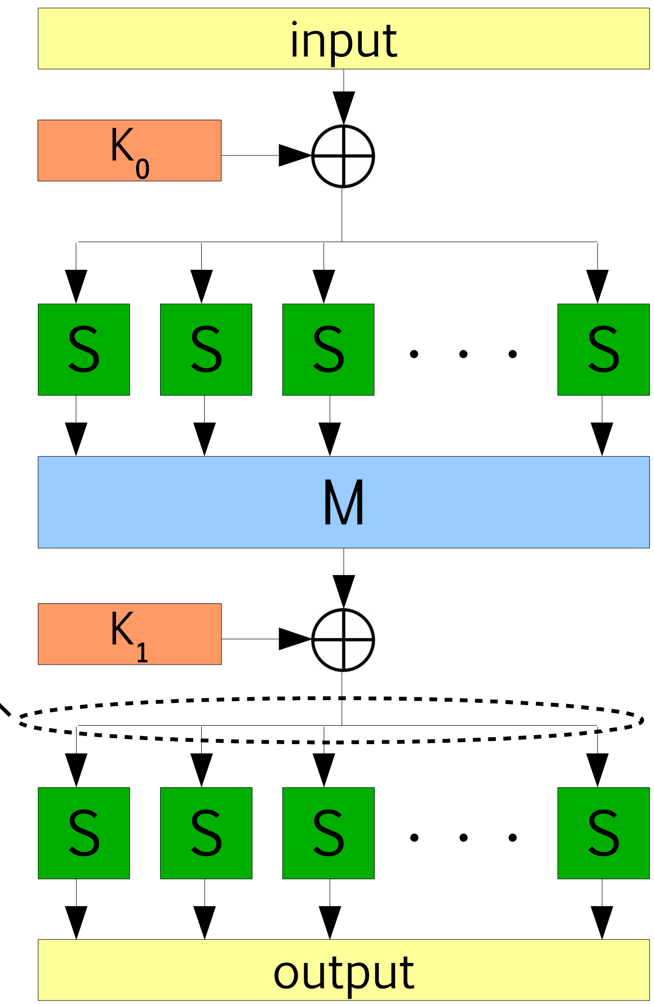
- we exploit structure to bound collision probabilities

# SP-network with random S-box

- Fix queries $x_1, \ldots, x_q \in \{0,1\}^n$.

- Pr [$\exists$ collision in any 2 final-round S-boxes]
  $\leq$ poly(m,q) $\cdot$ $2^{-b}$.
  - uses M invertible, all entries $\neq 0$
  - non-trivial for $x_i \neq x_j$, same S-box

- No collisions $\Longrightarrow$ output is uniform.



# Outline

Introduction

SP-network: definition and security

New PRF candidates

SP-network with random S-box

**Natural Proofs**

# Natural Proofs [Razborov-Rudich '97]

- CKT = any complexity class (e.g. circuits of size $n^2$)

- Observation: Most lower bounds against CKT distinguish CKT truth tables from random truth tables.

- Implication: If CKT can compute $2^{-n}$-secure PRF, most techniques can't prove CKT lower bounds.

- Gap:

| | | |
|---|---|---|
| best PRF: | size $\Omega(n^2)$ | [Naor-Reingold '04] |
| best lower bound: | size $O(n)$ | [Blum '84] |

# Natural Proofs [Razborov-Rudich '97]

- CKT = any complexity class (e.g. circuits of size $n^2$)

- Observation: Most lower bounds against CKT distinguish CKT truth tables from random truth tables.

- Implication: If CKT can compute $2^{-n}$-secure PRF, most techniques can't prove CKT lower bounds.

- We narrow the gap in 3 models (if our PRF $2^{-n}$-secure).
  - Boolean circuits of size $n \cdot \log^{O(1)}(n)$
  - $TC^0$ circuits of size $O(n^{1+\varepsilon})$ for any $\varepsilon > 0$ [Allender-Koucký '10]
  - time-$O(n^2)$ 1-tape Turing machines

# Conclusion

## SPN structure underexplored for PRF

- lends itself to efficient circuits
- combinatorial hardness, vs. algebraic for complexity PRF
- we give evidence that SPNs are plausible PRF candidates
- we provide asymptotic analysis of SPN structure

## Future directions

- simplest, most efficient possible PRF?
  - linear-size circuits
  - branching programs
  - communication protocols
  - ...
- analyze our PRF candidates against other attacks