Sometimes-Recurse Shuffle

Almost-Random Permutations in Logarithmic Expected Time

Ben Morris
Dept. of Mathematics
UC Davis, USA

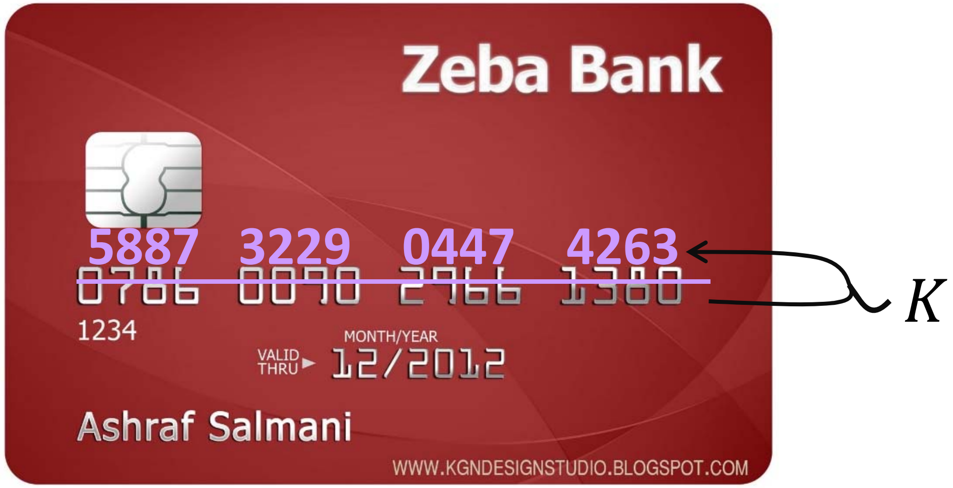
Phillip Rogaway
Dept. of Computer Science
UC Davis, USA

13 May 2014

EUROCRYPT 2014
Copenhagen, Denmark

Enciphering a Credit-Card Number

(also called a "PAN")



$$E\colon\ \breve{}\ \times \{0,1,\ldots,9\}^{16} \to \{0,1,\ldots,9\}^{16}$$

Format-Preserving Encryption (FPE): ← named & popularized by **T. Spies**

[NBS FIPS 74: 1981]

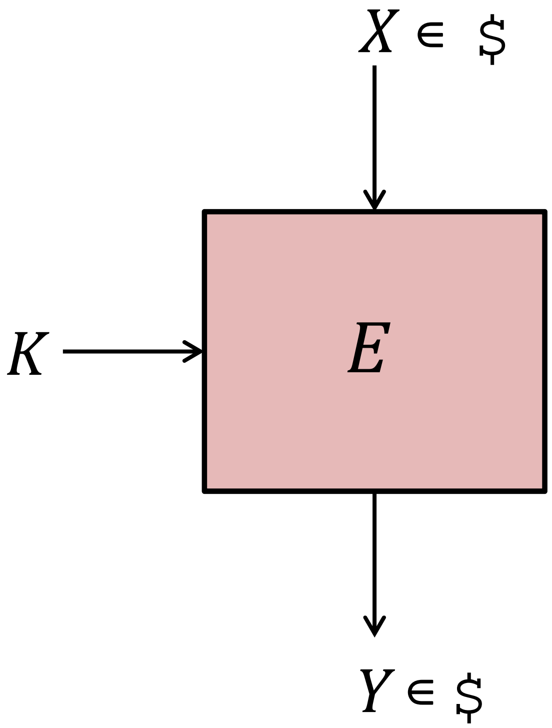
$$E\colon\ \breve{}\ \times \$\, y\!\!\to\ \$$$

FPE $\overset{?}{=}$ Blockcipher

Sort of

$E\colon\ \breve{}\ \times \$\, \text{y}\!\to\ \$$

$E(K,\cdot)$ is a permutation on \$



Assumption: $\$\ = [N] = \{0, \ldots, N-1\}$

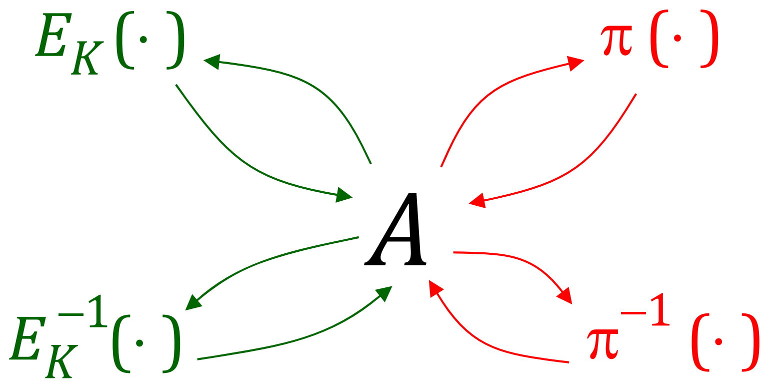
Not *that* limiting – many natural messages spaces can be efficiently put into 1-to-1 correspondence with $[N]$

[Black, Rogaway 2002]

[Bellare, Ristenpart, Rogaway, Stegers 2009]

Measuring quality

$E\colon \breve{\ } \times \$ \rightarrow \$$



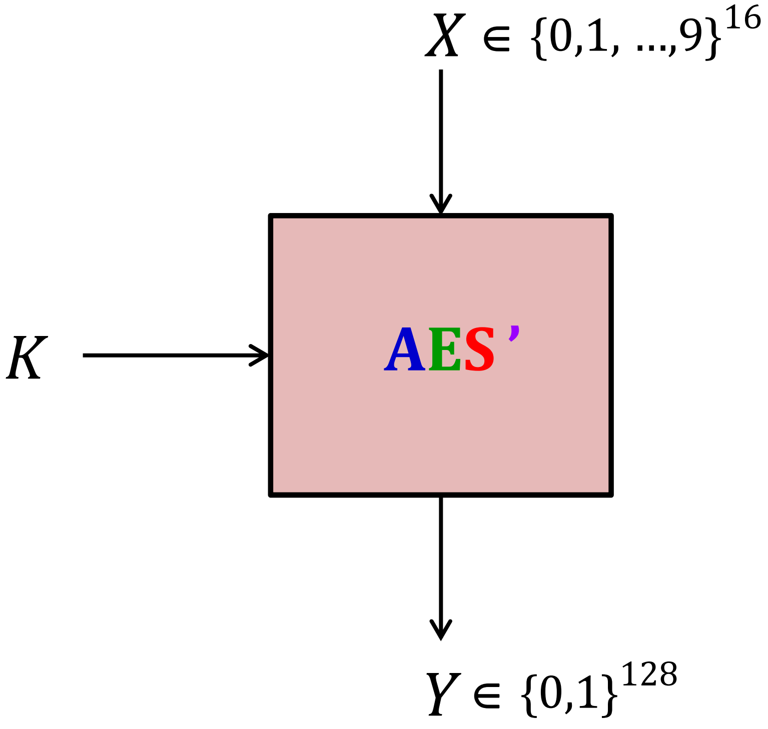
$$\boxed{\mathbf{Adv}_E^{\mathrm{sprp}}(q) = \max_{A \text{ asks } q \text{ queries}} \Pr[A^{E_K \; E_K^{-1}} \rightarrow 1] - \Pr[A^{\pi \; \pi^{-1}} \rightarrow 1]}$$

$$\boxed{\Delta_E(q) = \max_{\substack{A \text{ asks } q \\ \text{nonadaptive queries}}} \Pr[A^{E_K} \rightarrow 1] - \Pr[A^{\pi} \rightarrow 1]}$$

When q=N
these coincide

One approach to FPE

De novo construction



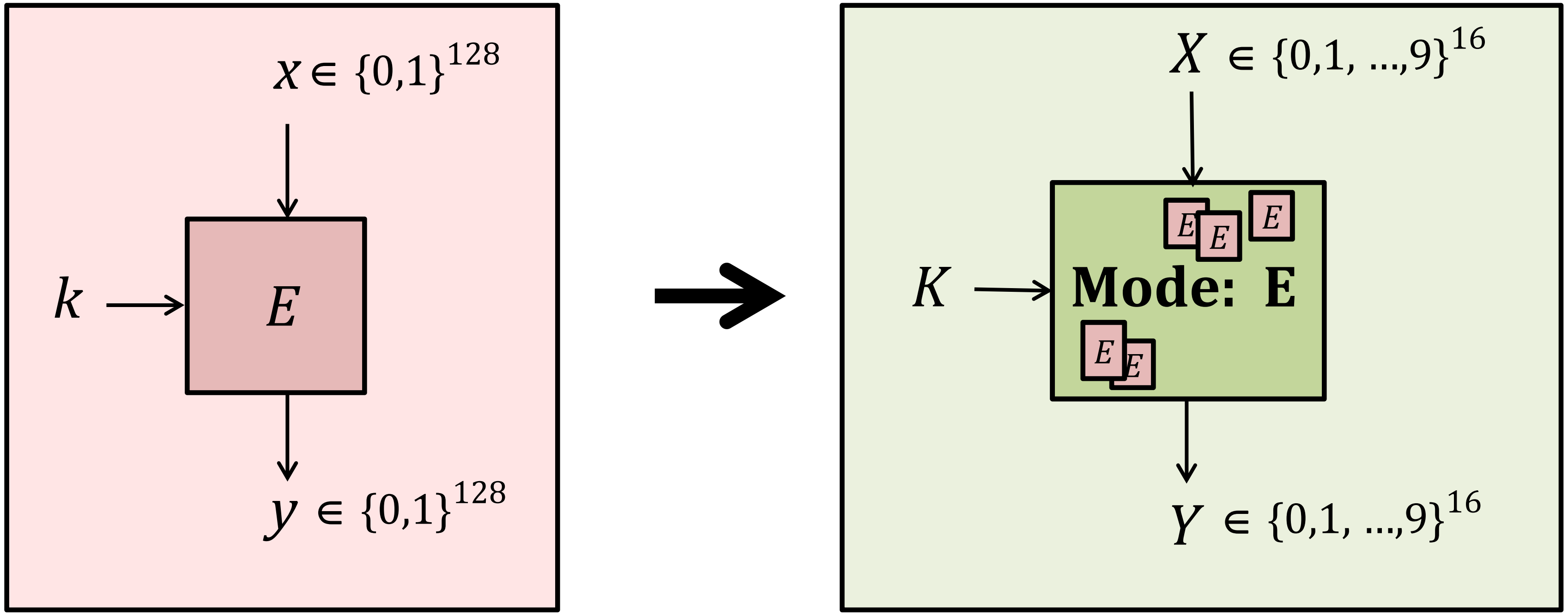
Lots of problems

- Unclear **how** to extend conventional blockciphers to small/unusual domains.
- **Security assurances** earned by existing blockcipher **forfeit**
- **Existing HW** and **SW** not exploitable

There exist designs that allow short binary strings, like **HPC**, but don't go as far as [*N*]

Another approach to FPE

PRF to PRP conversion



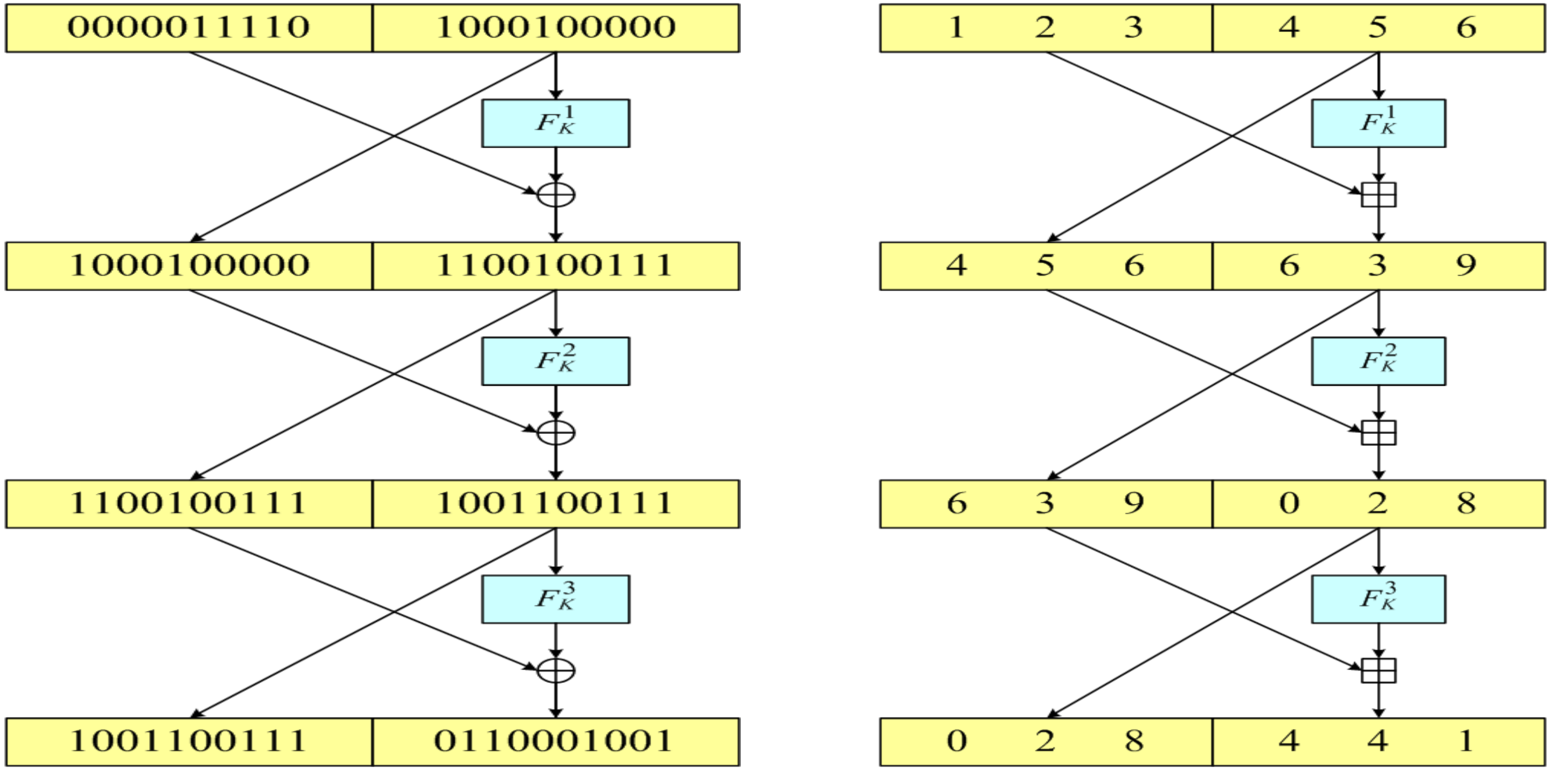
PRP with a domain $\{0,1\}^b$ → **PRP** with a domain $[N]$

PRF with a domain $\{0,1\}^b$ → **PRP** with a domain $[N]$

Random function with domain $\{0,1\}^b$ → Random permutation with domain $[N]$

That’s what Feistel does

Random function with domain $\{0,1\}^b$ → Random permutation with domain $[N]$



Poor concrete security

Luby-Rackoff: proven security to $q \sim N^{1/4}$

Patarin: provable security to $q \sim N^{1/2}$

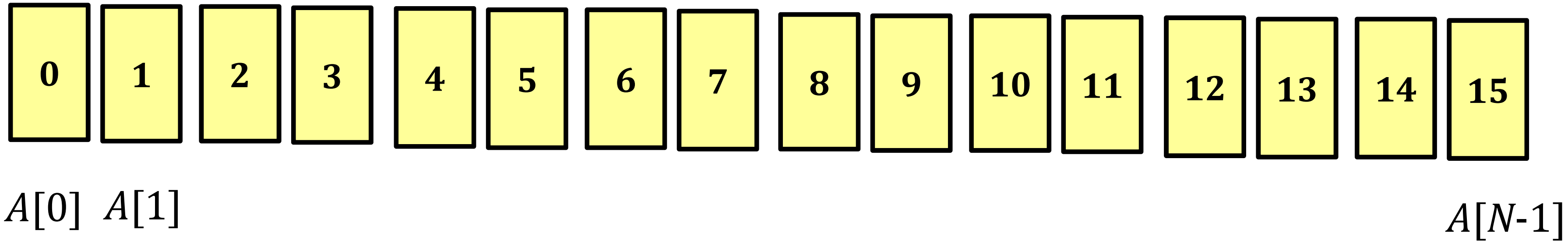
Folklore: inf th attacks to $q \sim N^{1/2}$

Goal: security to $q = N$

full security **[Ristenpart, Yilek 2013]**

Full security <u>is</u> feasible

At least if you spend $\Omega(N)$ time



```
for $j$ from $0$ to $N-1$ do $A[i] \leftarrow i$
for $j$ from $N-1$ downto $1$ do
    $i \twoheadleftarrow [\,j\,]$
    $A[i] \leftrightarrow A[j]$
```

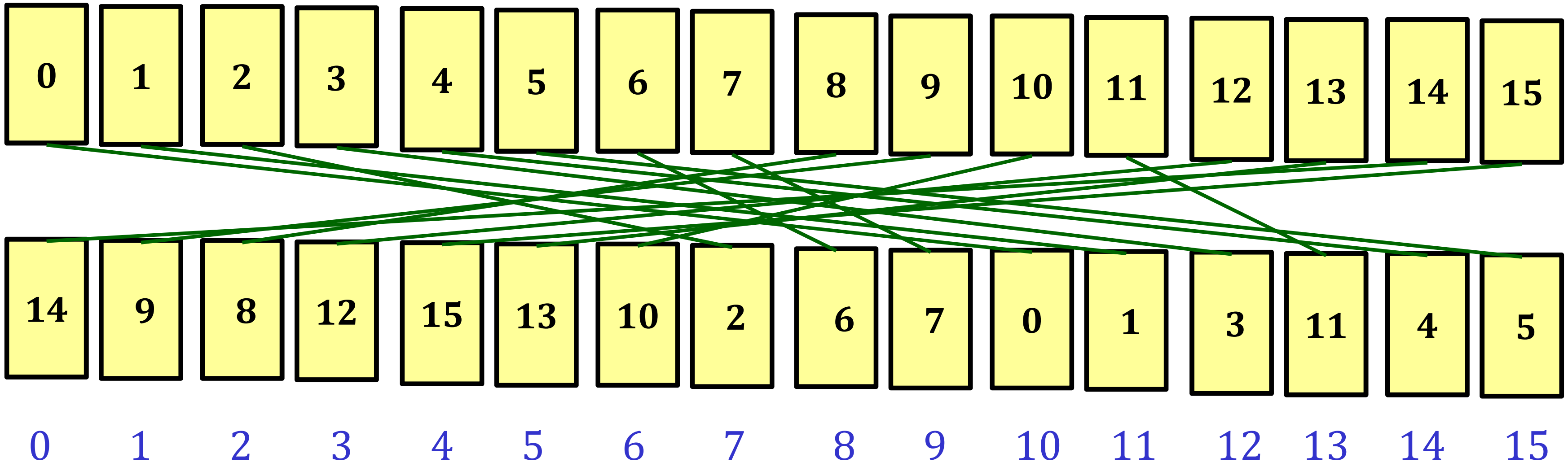
Let key K name these choices: sequence of numbers in $[N]$, $[N-1]$, …,$[3]$, $[2]$, $[1]$

“Knuth Shuffle”

(Fisher-Yates)

The Route Towards Better Methods/Bounds

Enciphering Scheme ↔ Card Shuffle

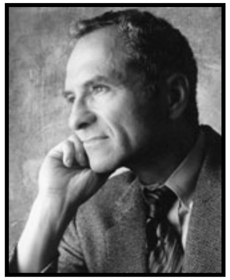


A point in x∈$ ↔ A particular card

A key K∈˘ y ↔ Randomness used to shuffle the cards

Image $E_K(x)$ ↔ Where that card ends up with the given randomness

An **oblivious** shuffle: can follow the path of a card without attending to the other cards. [Naor, 1989]



[Thorp 1973]

Thorp Shuffle

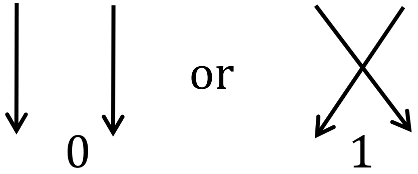
TH$[N, r]$

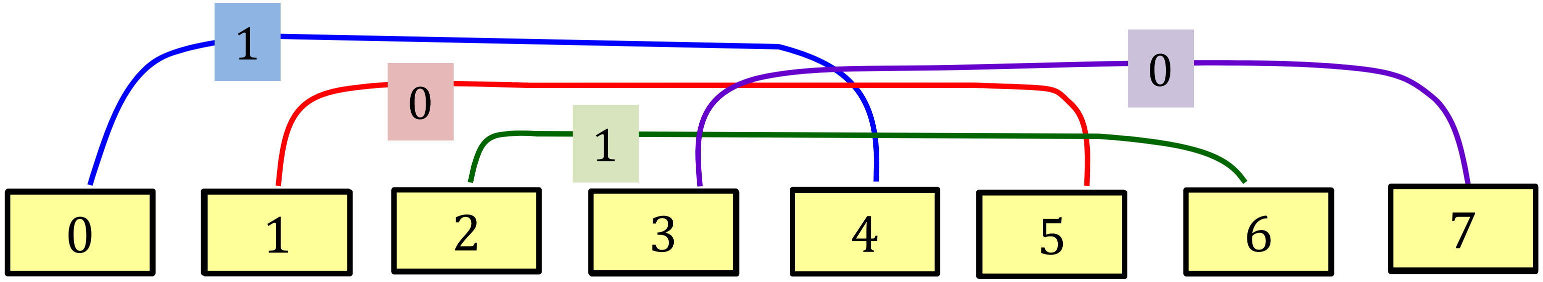
repeat r times

1. Pair cards at posns x and $x + N/2$

2. Flip a coin for each pair

3. The coins indicate if pairs go

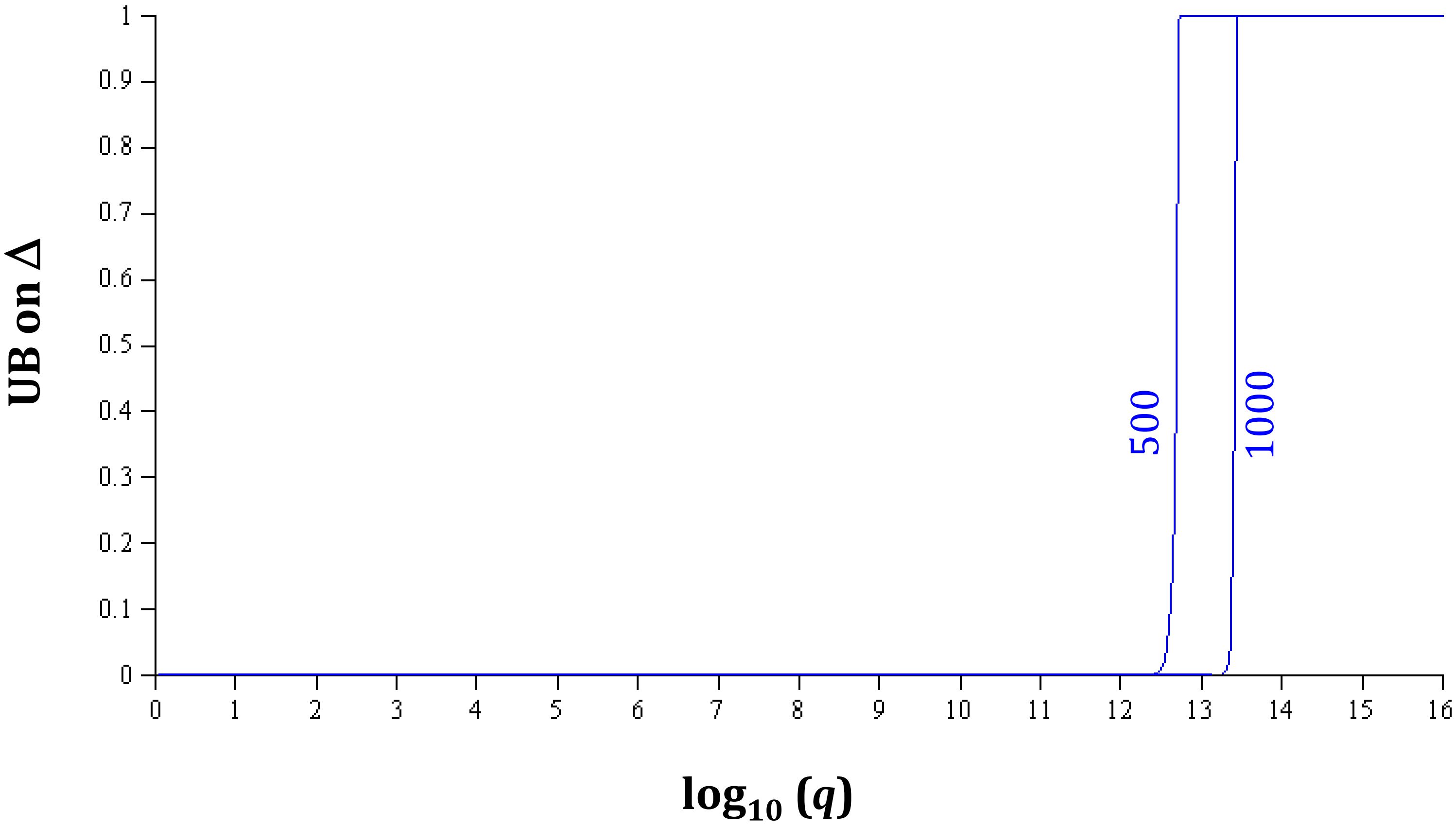




Security of Thorp

TH$[10^{16}, r]$

[Morris, Rogaway, Stegers 2009]
[Hoang, Rogaway 2010]



Swap-or-Not SN[N, r]

[Hoang, Morris, Rogaway 2012]

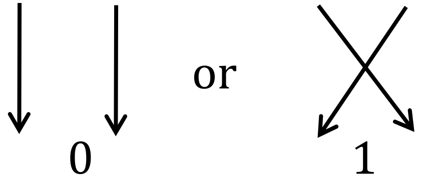
repeat r times

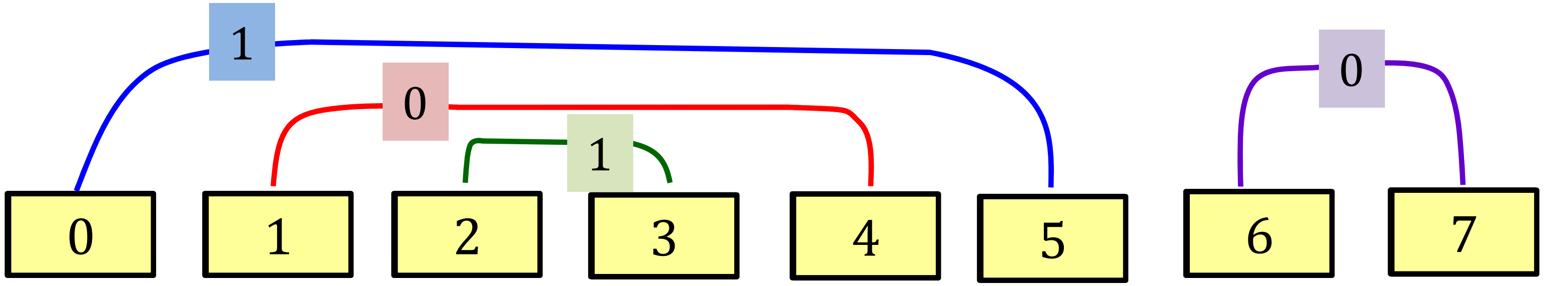
1. $K \twoheadleftarrow [N]$ Eg, $K = 5$ below

2. Pair x and $K{-}x \pmod{N}$

3. Flip a coin for each pair

4. The coins indicate if pairs go





Swap-or-Not SN[N, r]

[Hoang, Morris, Rogaway 2012]

As a **blockcipher**

```
**algorithm** $E_{K_1 \ldots K_R\ F}(x)$    // $x \in \{0, \ldots, N-1\}$
**for** $i \leftarrow 1$ **to** $r$ **do**
        $x' \leftarrow K_i - x$
        $x^* \leftarrow \max(x, x')$
        **if** $F(i, x^*) = 1$ **then** $x \leftarrow x'$
**return** $x$
```

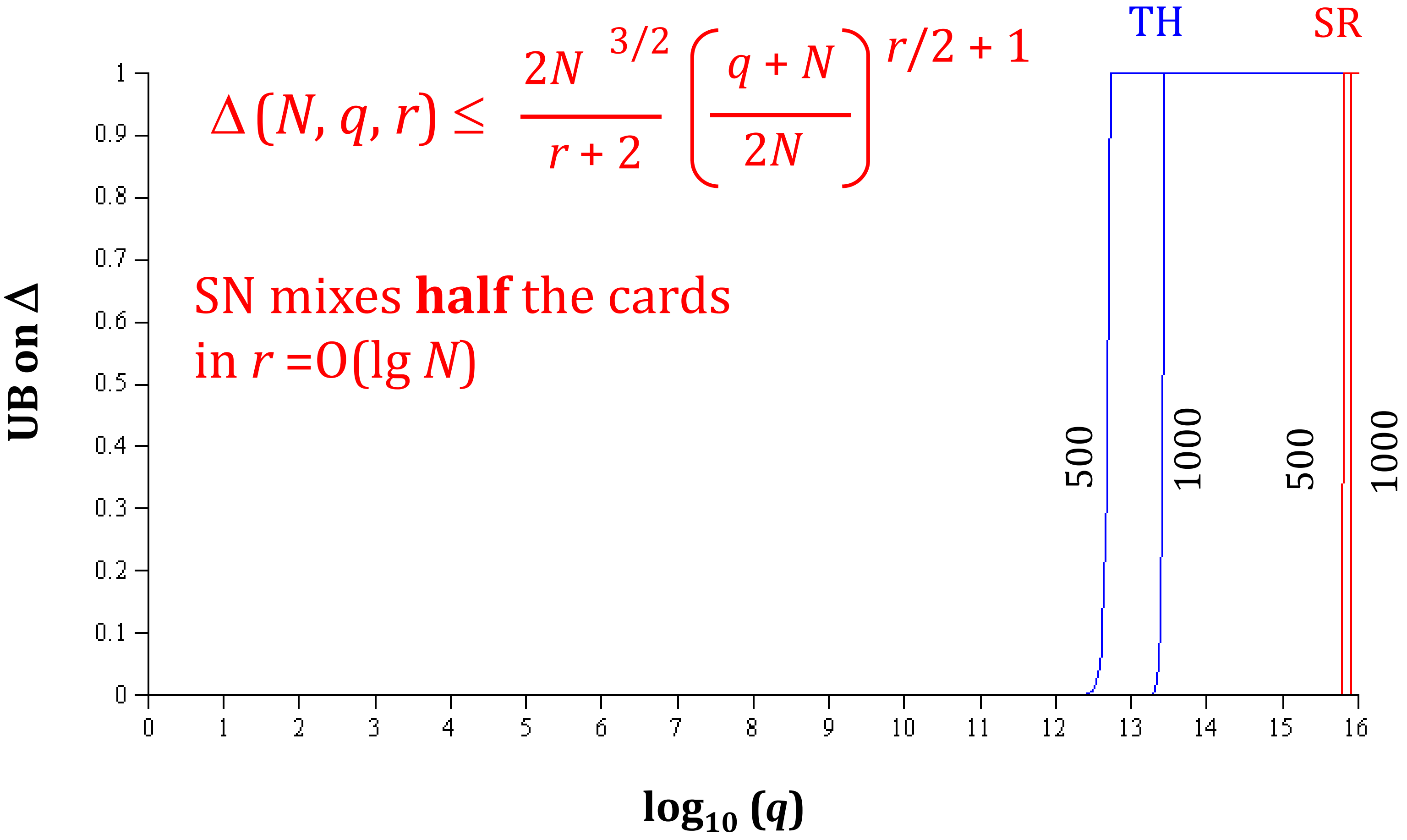
Decryption: Same, with *i* going from *r* downto 1

Bounds for SN apply to SN^{-1}

[Hoang, Morris, Rogaway 2012]

Security of Swap-or-Not

SN$[10^{16}, r]$



$$\Delta(N, q, r) \le \frac{2N^{3/2}}{r+2}\left(\frac{q+N}{2N}\right)^{r/2+1}$$

SN mixes **half** the cards in $r = O(\lg N)$

Bootstrapping an inner shuffle

Icicle & Mix-and-Cut

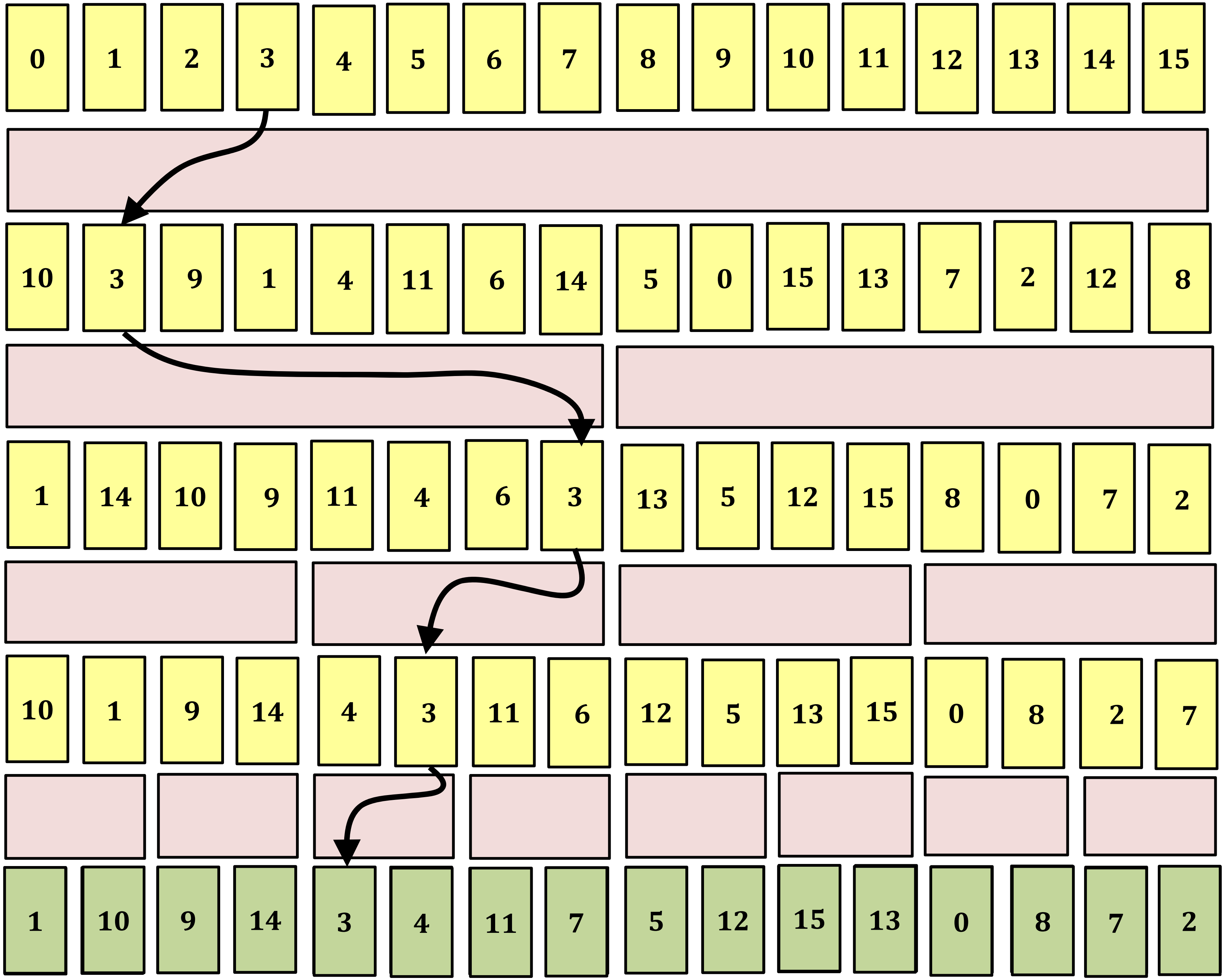
[Ristenpart, Yilek 2013]
following
[Granboulan-Pornin 2007] and
[Czumaj, Kanarek, Kutylowski and 1998]

- Apply some inner shuffle.
  It needs to be a pseudorandom separator (PRS):
  the set of elements in the left & right output pile should be near uniform
- Recurse down left & right output piles

Icicle

- Use SN[N, O(lg N)] is a PRS
- Total time: $O(\lg^2 N)$

Mix-and-Cut

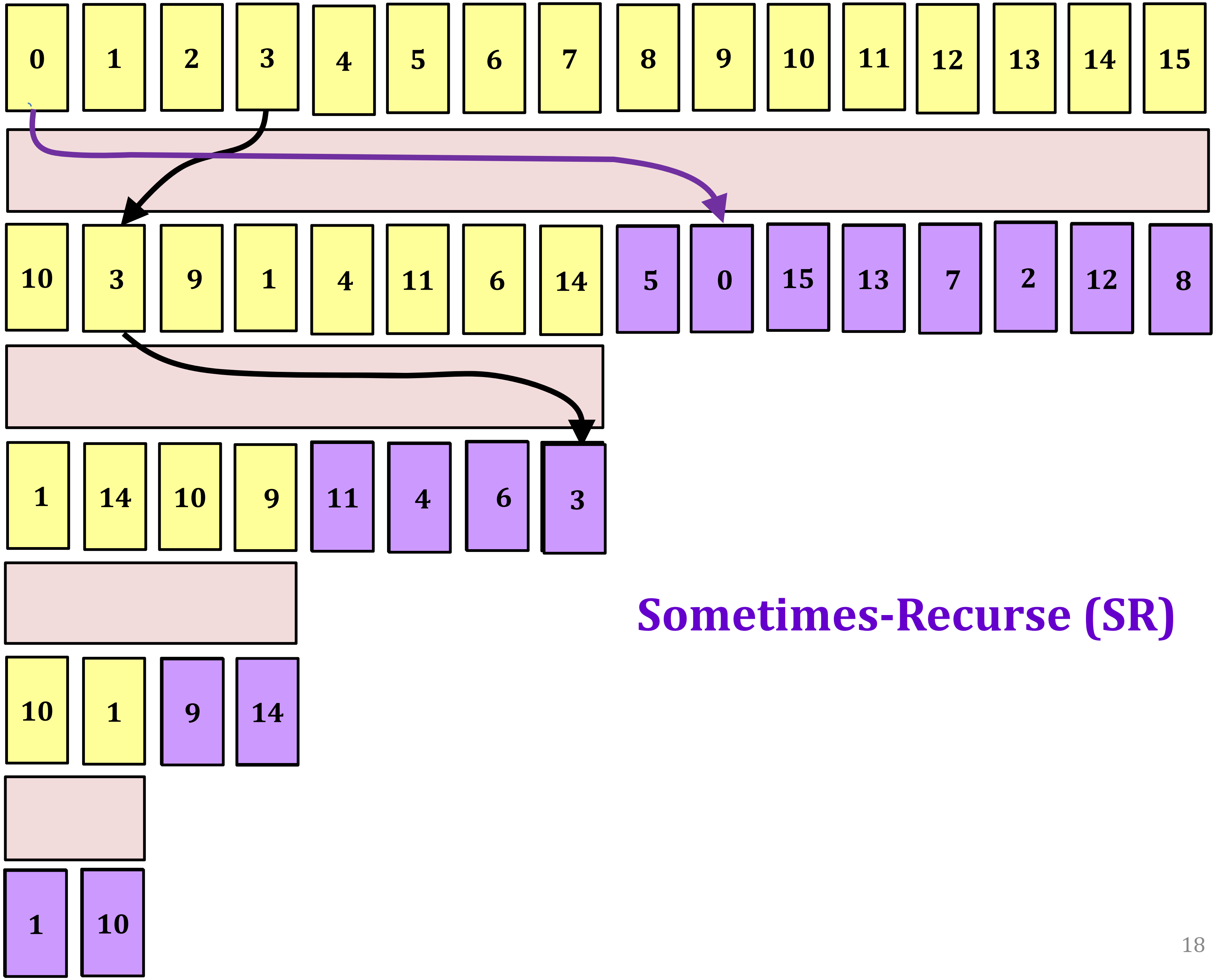

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
10 3 9 1 4 11 6 14 5 0 15 13 7 2 12 8
1 14 10 9 11 4 6 3 13 5 12 15 8 0 7 2
10 1 9 14 4 3 11 6 12 5 13 15 0 8 2 7
1 10 9 14 3 4 11 7 5 12 15 13 0 8 7 2

Sometimes-Recurse (SR) Shuffle

- Apply some inner shuffle.
  It needs to mix **half** the cards (in the inverse shuffle):
- Recurse down **one** of the two output piles – the **left**, say

Anticipated instantiation:

- Use SN[N, O(lg *N*)] as the inner shuffle



Sometimes-Recurse (SR)

SR as a Blockcipher

```
algorithm $E^{N}_{K,F}(x)$      // $x \in \{0, \ldots, N-1\}$
if $N$=1 then return $x$

for $i \leftarrow 1$ to $r_N$ do
        $x' \leftarrow K_i - x$
        $x^* \leftarrow \max(x, x')$                 SN($N$, $r_N$)
        if $F(i, x^*)=1$ then $x \leftarrow x'$

if $x \le N/2$ then return $E^{\lfloor N/2 \rfloor}_{K,F}(x)$
                else return $x$
```

With appropriate r_N
full security in O(lg N) **expected** rounds

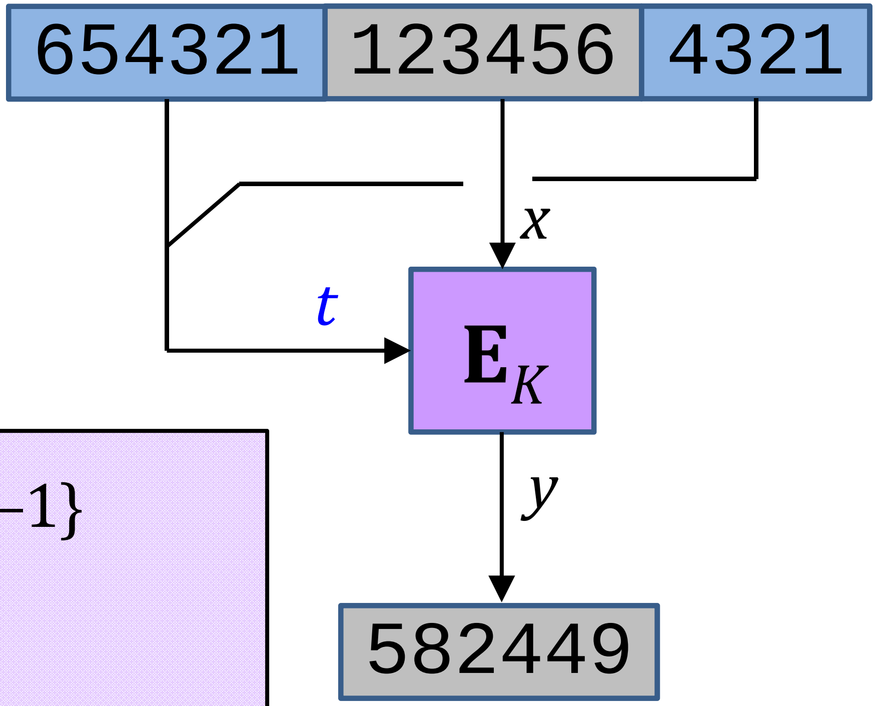
Number of rounds

error to ε = 10^{-10}

Plaintext	Best	Expected	Worst	r_N
6-digits	289	**563**	4411	fixed
	272	**544**	5168	splits ε
16-digits	531	**1048**	18239	fixed
About 80k cycles, 25 μsec	507	**1014**	26365	splits ε
30-digits	869	**1723**	51453	fixed
	840	**1680**	83160	splits ε

Supporting Tweaks

[Liskov, Rivest, Wagner 2002]



```
algorithm $E^{N}_{K,F}(x)$      // $x \in \{0, \ldots, N-1\}$
if $N$=1 then return $x$

for $i \leftarrow 1$ to $r_N$ do
        $x' \leftarrow K_i - x$
        $x^* \leftarrow \max(x, x')$
        if $F(i, x^*, t)$=1 then $x \leftarrow x'$

if $x \le N/2$ then return $E^{\lfloor N/2 \rfloor}_{K,F}(x)$
          else return $x$
```

Doesn't need to depend on t

Choosing the split

Not necessary to choose |Left| = $\lfloor N/2 \rfloor$

Plaintext	**Expected**	$\lvert\text{Left}\rvert$	$\boldsymbol{r_N}$
16-digits	~~**1014**~~ 1010	$\lfloor 0.52\ N/2 \rfloor$	splits ε

Makes little difference

A Potential Concern

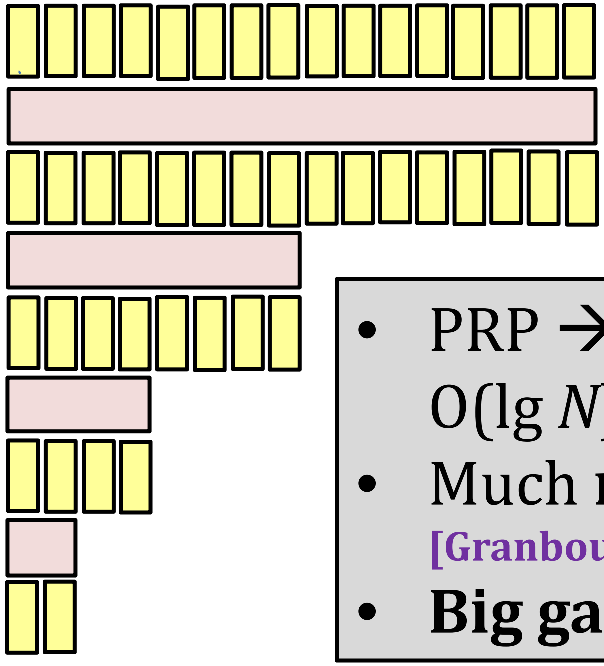
Leaking the runtime

```
algorithm $E^{N}_{K,F}(x)$    // $x \in \{0, \ldots, N-1\}$
if $N$=1 then return $x$

for $i \leftarrow 1$ to $r_N$ do
        $x' \leftarrow K_i - x$
        $x^* \leftarrow \max(x, x')$                  } $\mathrm{SN}(N, r_N)$
        if $F(i, x^*)$=1 then $x \leftarrow x'$

if $x \leq N/2$ then return $E^{\lfloor N/2 \rfloor}_{K,F}(x)$
                 else return $x$
```

Not an issue – the number of repetitions used to encipher x is already revealed by the ciphertext y



Summary

- PRP → PRP, for any [N], with **full security**, in O(lg N) **expected** time
- Much **more efficient** than prior work
  [Granboulan-Pornin 2007], [Stefanov-Shi 2012], [Ristenpart, Yilek 2012]
- **Big gap** to practice remains: r =10 *vs.* r =1000

Open

- O(lg N) **worst-case** time?