Smashing WEP in A Passive Attack

POUYAN SEPEHRDAD
PETR SUSIL
SERGE VAUDENAY
MARTIN VUAGNOUX

No one Uses **WEP**

Any More.

Hotels

No one Uses **WEP**

Any More.

Restaurants

Airports

Hotels

Wireless Networks in Singapore: 20% WEP

No one Uses WEP Any More.

Restaurants

Singapore is not alone.
The same problem in most Asia.

RC4

RC4

Reminder on RC4

RC4

Reminder on RC4

RC4/WEP

RC4

Reminder on RC4

RC4/WEP

Tornado Attack on WEP

RC4

Reminder on RC4

RC4/WEP

Tornado Attack on WEP

Challenges

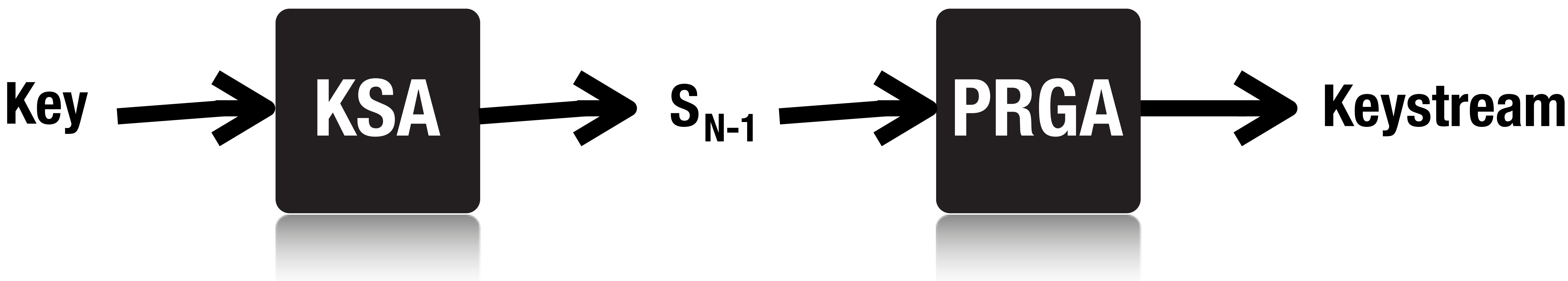
RC4

Reminder on RC4

RC4/WEP

Tornado Attack on WEP

Challenges


Key
KSA
S_{N-1}
PRGA
Keystream

```
for i = 0 to N − 1 do
    S[i] ← i
end for
j ← 0
for i = 0 to N − 1 do
    j ← j + S[i] + K[i mod L]
    swap(S[i], S[j])
end for
```

KSA

for $i = 0$ to $N - 1$ **do**
  $S[i] \leftarrow i$
end for
$j \leftarrow 0$
for $i = 0$ to $N - 1$ **do**
  $j \leftarrow j + S[i] + K[i \bmod L]$
  $\mathrm{swap}(S[i], S[j])$
end for

KSA

0	1	2	3	4	5	6	7	8	9	10	11	12	...	255
i							j							

```
for i = 0 to N − 1 do
    S[i] ← i
end for
j ← 0
for i = 0 to N − 1 do
    j ← j + S[i] + K[i mod L]
    swap(S[i], S[j])
end for
```

KSA

7	1	2	3	4	5	6	0	8	9	10	11	12	...	255
i							j							

```
for i = 0 to N − 1 do
    S[i] ← i
end for
j ← 0
for i = 0 to N − 1 do
    j ← j + S[i] + K[i mod L]
    swap(S[i], S[j])
end for
```

KSA

7	1	2	3	4	5	6	0	8	9	10	11	12	...	255
	i											j		

```
for i = 0 to N − 1 do
    S[i] ← i
end for
j ← 0
for i = 0 to N − 1 do
    j ← j + S[i] + K[i mod L]
    swap(S[i], S[j])
end for
```

KSA

7	12	2	3	4	5	6	0	8	9	10	11	1	...	255
	i											j		

```
i ← 0
j ← 0
loop
    i ← i + 1
    j ← j + S[i]
    swap(S[i], S[j])
    output z_i = S[S[i] + S[j]]
end loop
```

PRGA

$i \leftarrow 0$
$j \leftarrow 0$
loop
  $i \leftarrow i+1$
  $j \leftarrow j+S[i]$
  $\mathrm{swap}(S[i], S[j])$
  output $z_i = S[S[i]+S[j]]$
end loop

PRGA

18	3	211	7	81	245	121	5	66	78	189	34	133	...	32
	i		j											

```
i ← 0
j ← 0
loop
    i ← i + 1
    j ← j + S[i]
    swap(S[i], S[j])
    output z_i = S[S[i] + S[j]]
end loop
```

PRGA

18	7	211	3	81	245	121	5	66	78	189	34	133	...	32
	i		j											

$i \leftarrow 0$
$j \leftarrow 0$
loop
  $i \leftarrow i + 1$
  $j \leftarrow j + S[i]$
  $\text{swap}(S[i], S[j])$
  output $z_i = S[S[i] + S[j]]$
end loop

PRGA

18	7	211	3	81	245	121	5	66	78	189	34	133	...	32
	i		j											

Keystream byte = S[7+3]=S[10]=189

RC4

Reminder on RC4

RC4/WEP

Tornado attack on WEP

Challenges

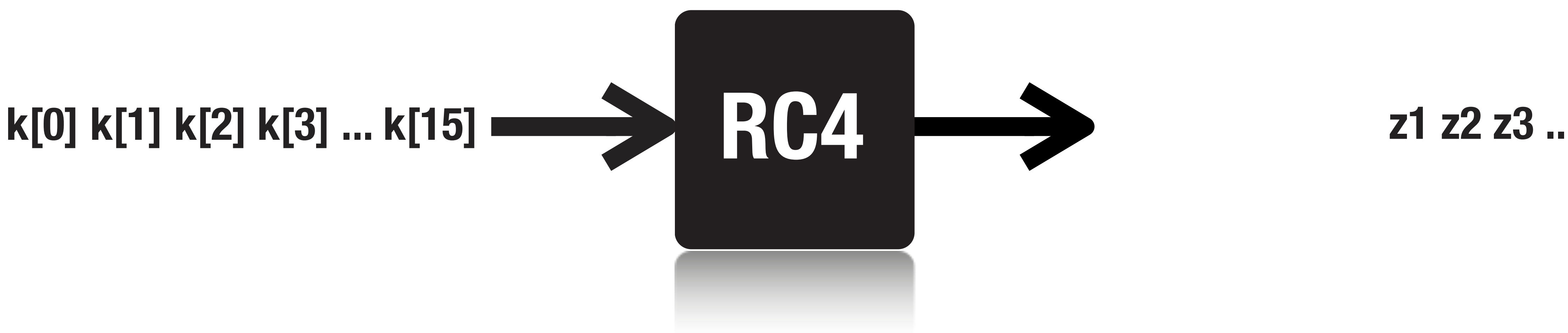
RC4

Reminder on RC4

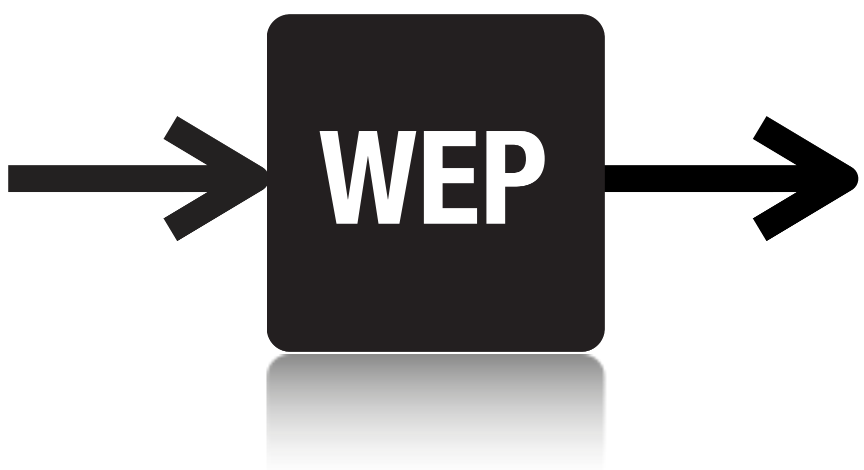
RC4/WEP

Tornado attack on WEP

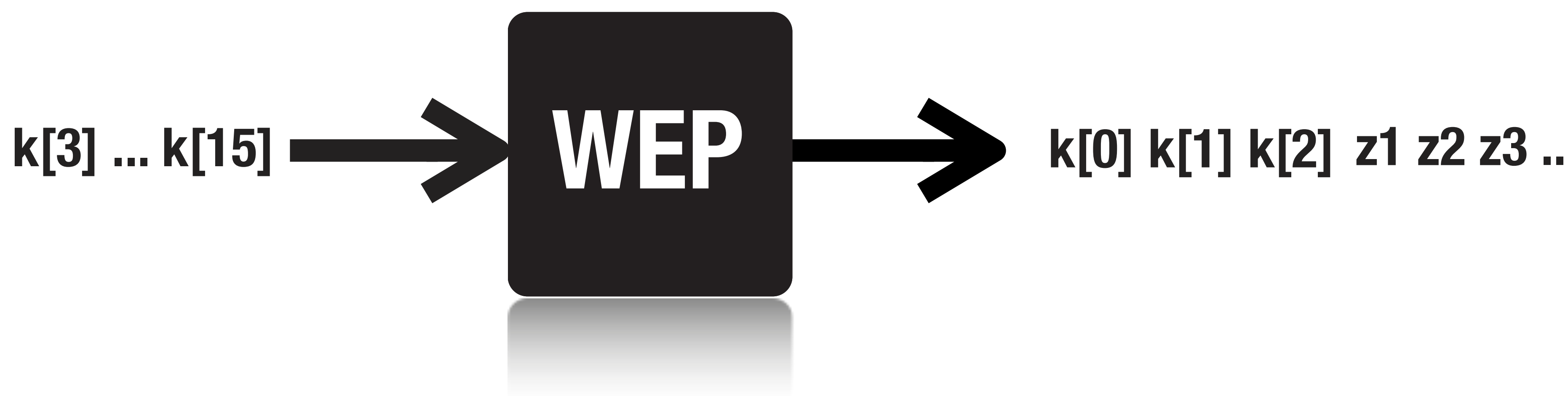
Challenges

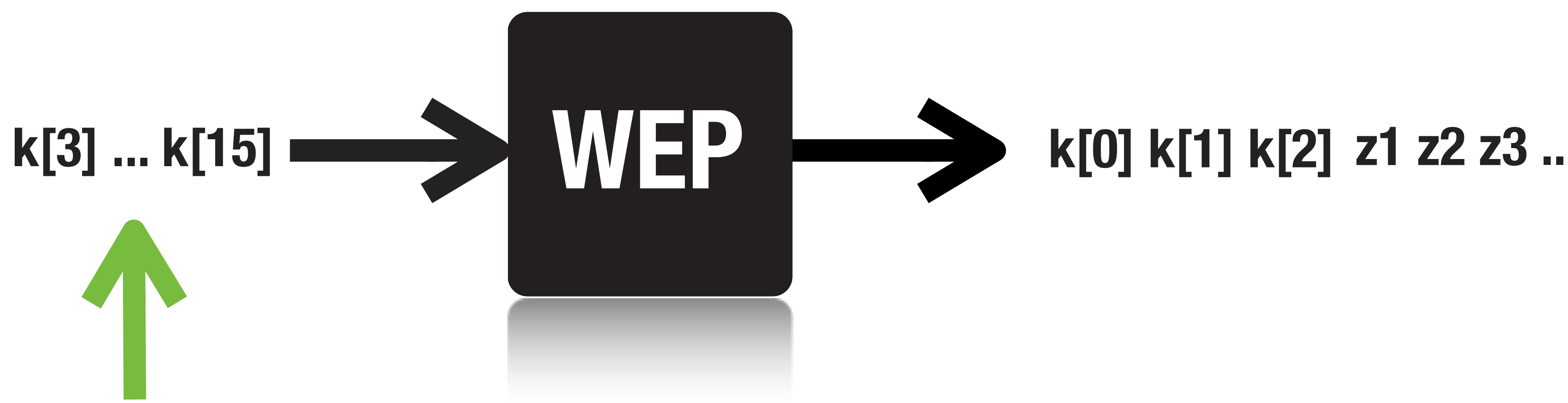

k[0] k[1] k[2] k[3] ... k[15]
RC4
z1 z2 z3 ...

k[0] k[1] k[2] k[3] ... k[15]



z1 z2 z3 ...


k[3] ... k[15]
WEP
k[0] k[1] k[2] z1 z2 z3 ...



the same for each packet encryption.

WEP is vulnerable.

RC4

Reminder on RC4

RC4/WEP

Tornado Attack on WEP

Challenges

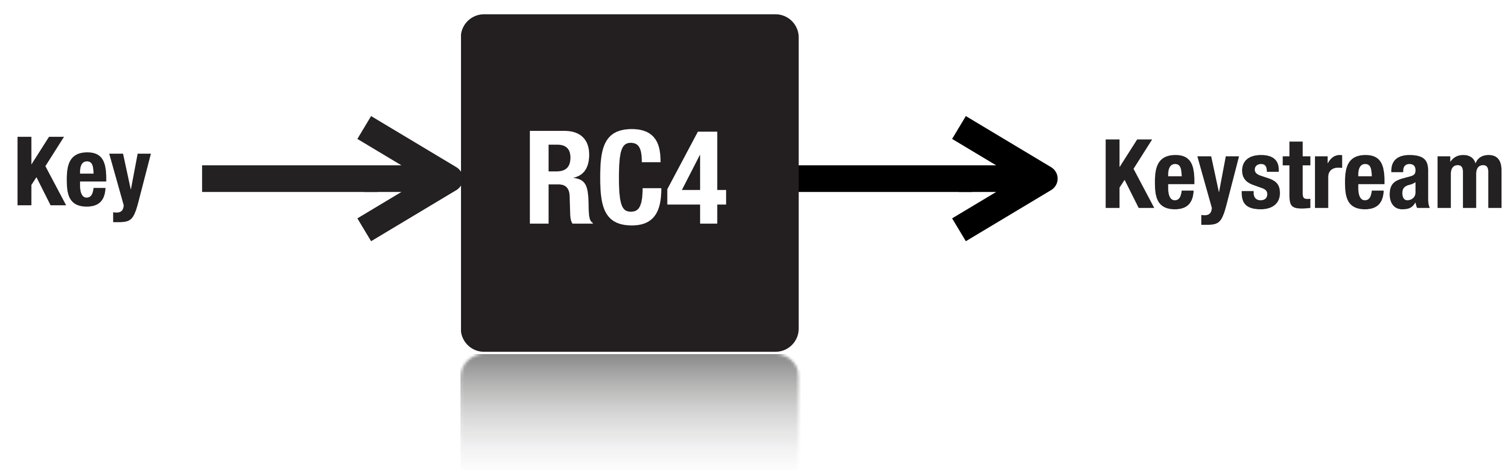
RC4

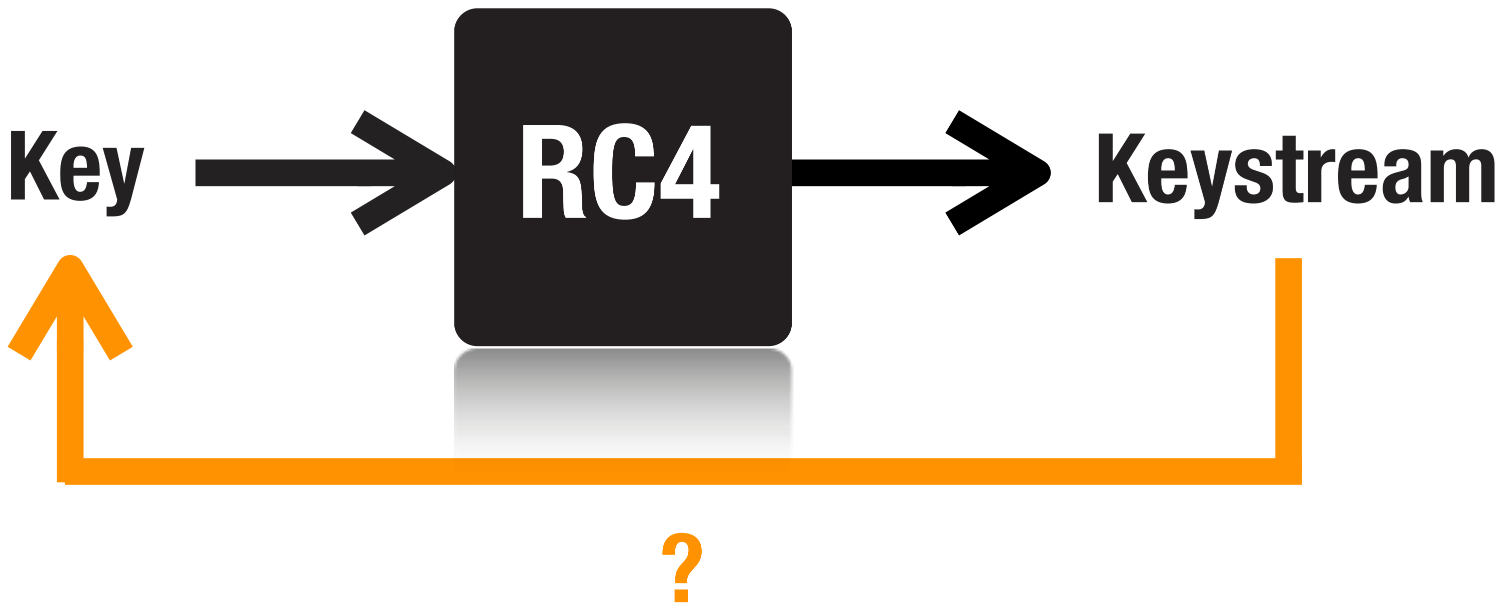
Reminder on RC4

RC4/WEP

Tornado Attack on WEP

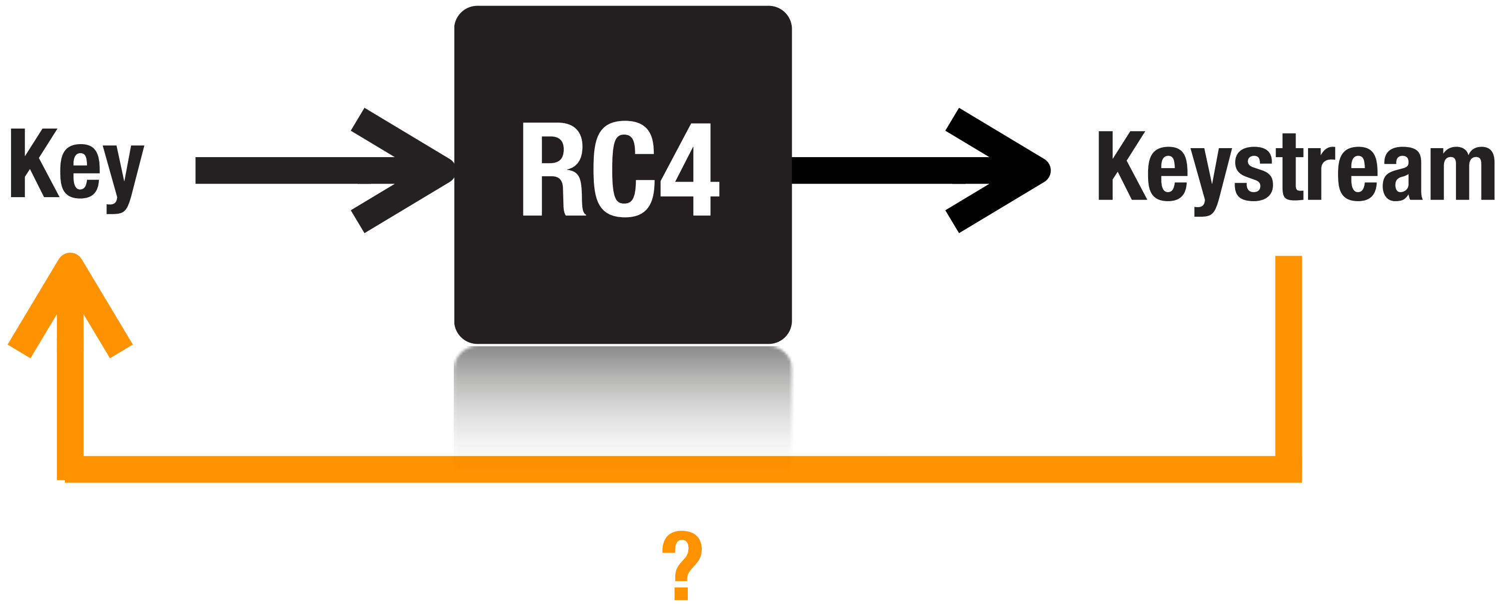
Challenges


Key
RC4
Keystream


Key
RC4
Keystream
?

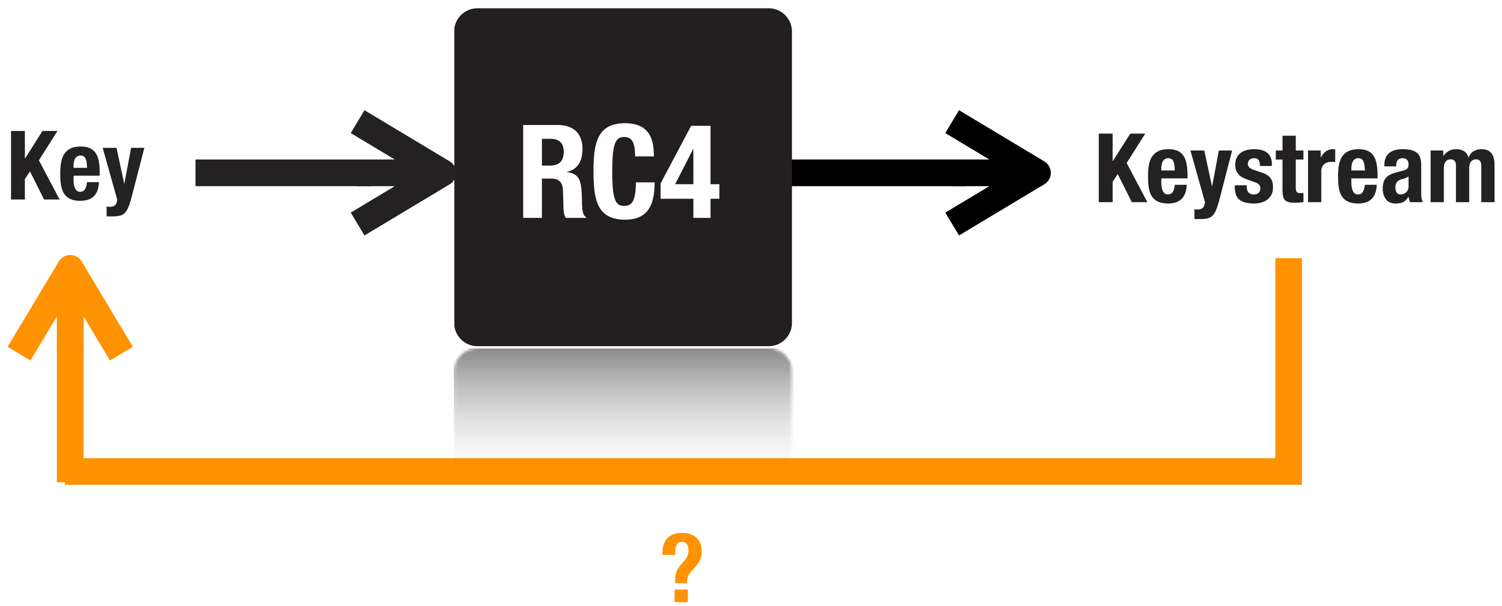
Conditional biases: pairs of $\bar{f}_j, p_j$ with a predicate $\bar{g}_j$

$$\Pr[\bar{K}[i] = \bar{f}_j(z, \mathrm{clue}) | \bar{g}_j(z, \mathrm{clue})] = p_j$$



Conditional biases: pairs of $\bar{\mathsf{f}}_\mathsf{j}, \mathsf{p}_\mathsf{j}$ with a predicate $\bar{\mathsf{g}}_\mathsf{j}$

$$\mathsf{Pr}[\bar{\mathsf{K}}[\mathsf{i}] = \bar{\mathsf{f}}_\mathsf{j}(\mathsf{z}, \mathsf{clue}) | \bar{\mathsf{g}}_\mathsf{j}(\mathsf{z}, \mathsf{clue})] = \mathsf{p}_\mathsf{j}$$

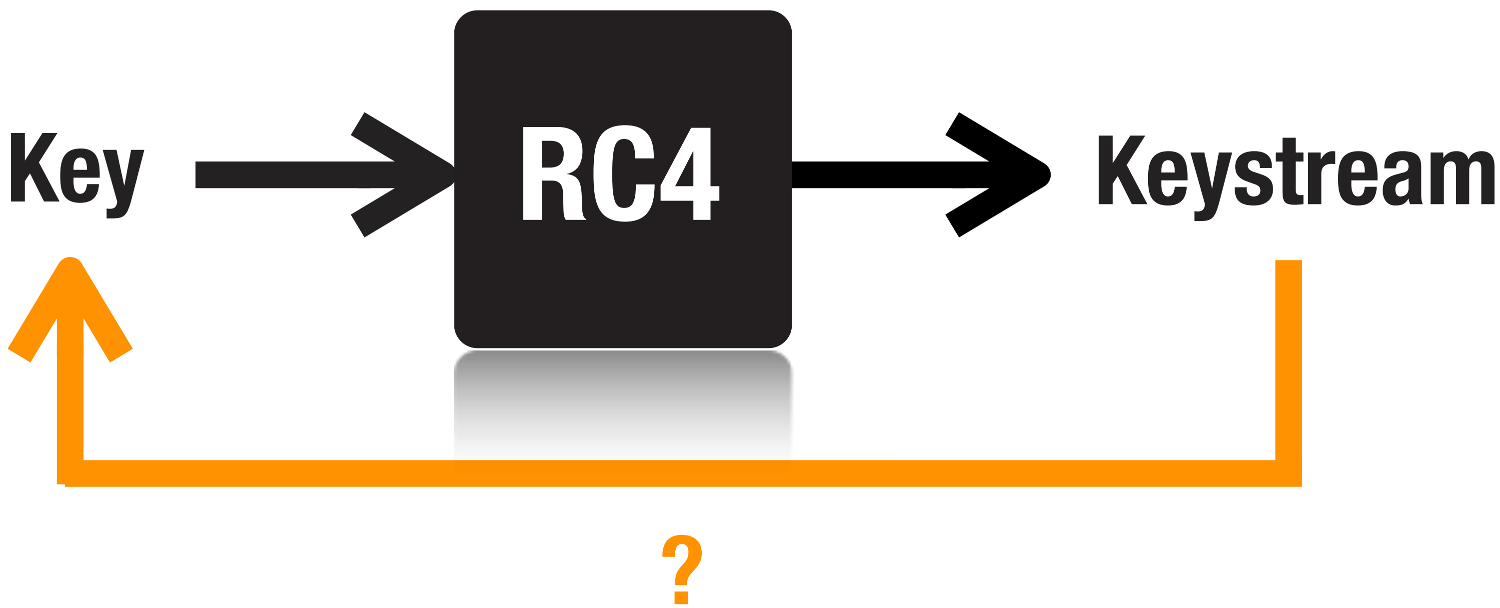


row	reference	$\bar{f}$	$\bar{g}$	p
i	A_u15	$2 - \sigma_i$	$S_t[i] = 0,\ z_2 = 0$	$P^1_{\mathsf{fixed}-j}$

Conditional biases: pairs of $\bar{f}_j, p_j$ with a predicate $\bar{g}_j$

$$\Pr[\bar{K}[i] = \bar{f}_j(z, \text{clue}) | \bar{g}_j(z, \text{clue})] = p_j$$

22 Biases



row	reference	$\bar{f}$	$\bar{g}$	p
i	A_u15	$2 - \sigma_i$	$S_t[i] = 0,\ z_2 = 0$	$P^1_{\text{fixed}-j}$

Roos, A.: A class of weak keys in RC4 stream cipher.
1995

Wagner, D.: Weak keys in RC4.
1995

Borisov, N., Goldberg, I., Wagner, D.: Intercepting mobile communications: the insecurity of 802.11.
2001

Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in the key scheduling algorithm of RC4.
2001

Stubblefield, A., Ioannidis, J., Rubin, A.D.: Using the Fluhrer, Mantin, and Shamir Attack to Break WEP.
2002

Korek: Next generation of WEP attacks?
2004

Devine, C., Otreppe, T.: Aircrack-ng
2004

Martin, J.I.S.: Weplab
2004

Mantin, I.: A practical attack on the fixed RC4 in the WEP mode.
2005

Klein, A.: Attacks on the RC4 stream cipher.
2006

Tews, E., Weinmann, R., Pyshkin, A.: Breaking 104 Bit WEP in Less Than 60 Seconds.
2007

Vaudenay, S., Vuagnoux, M.: Passive–only Key Recovery Attacks on RC4
2007

Beck, M., Tews, E. Practical Attacks Against WEP and WPA.
2009

Sepehrdad, P., Susil, P., Vaudenay, S., Vuagnoux, M.: Smashing WEP in a Passive Attack
2013

Roos, A.: A class of weak keys in RC4 stream cipher.
1995

Wagner, D.: Weak keys in RC4.
1995

Borisov, N., Goldberg, I., Wagner, D.: Intercepting mobile communications:
the insecurity of 802.11.
2001

Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in the key scheduling algorithm of RC4.
2001

Stubblefield, A., Ioannidis, J., Rubin, A.D.: Using the Fluhrer, Mantin, and Shamir Attack to Break WEP.
2002

5500,000

Korek: Next generation of WEP attacks? *100,000*
2004

Devine, C., Otreppe, T.: Aircrack-ng
2004

Martin, J.I.S.: Weplab
2004

Mantin, I.: A practical attack on the fixed RC4 in the WEP mode.
2005

Klein, A.: Attacks on the RC4 stream cipher. *60,000*
2006

Tews, E., Weinmann, R., Pyshkin, A.: Breaking 104 Bit WEP in Less Than 60 Seconds. *40,000*
2007

Vaudenay, S., Vuagnoux, M.: Passive–only Key Recovery Attacks on RC4 *32,700*
2007

Beck, M., Tews, E. Practical Attacks Against WEP and WPA. *30,000*
2009

Sepehrdad, P., Susil, P., Vaudenay, S., Vuagnoux, M.: Smashing WEP in a Passive Attack **19,800**
2013

Attack on WEP

compute the ranking $\mathcal{L}_{15}$ for $I = (15)$ and $I_0 = \{0, 1, 2\}$
truncate $\mathcal{L}_{15}$ to its first ρ_{15} terms
for each $\bar{k}_{15}$ in $\mathcal{L}_{15}$ **do**
    run recursive attack on input $\bar{k}_{15}$
end for
stop: attack failed

recursive attack with input $(\bar{k}_{15}, \bar{k}_3, \ldots, \bar{k}_{i-1})$**:**

If input is only $\bar{k}_{15}$, set $i = 3$.
if $i \leq i_{\max}$ **then**
    compute the ranking $\mathcal{L}_i$ for $I = (i)$ and $I_0 = \{0, \ldots, i-1, 15\}$
    truncate $\mathcal{L}_i$ to its first ρ_i terms
    for each $\bar{k}_i$ in $\mathcal{L}_i$ **do**
        run recursive attack on input $(\bar{k}_{15}, \bar{k}_3, \ldots, \bar{k}_{i-1}, \bar{k}_i)$
    end for
else
    for each $\bar{k}_{i_{\max}+1}, \ldots, \bar{k}_{14}$ **do**
        test key $(\bar{k}_3, \ldots, \bar{k}_{14}, \bar{k}_{15})$ and stop if correct
    end for
end if

Attack on WEP

compute the ranking $\mathcal{L}_{15}$ for $I = (15)$ and $I_0 = \{0, 1, 2\}$
truncate $\mathcal{L}_{15}$ to its first ρ_{15} terms
for each $\bar{k}_{15}$ in $\mathcal{L}_{15}$ **do**
    run recursive attack on input $\bar{k}_{15}$
end for
stop: attack failed

recursive attack with input $(\bar{k}_{15}, \bar{k}_3, \ldots, \bar{k}_{i-1})$**:**

If input is only $\bar{k}_{15}$, set $i = 3$.
if $i \leq i_{\max}$ **then**
    compute the ranking $\mathcal{L}_i$ for $I = (i)$ and $I_0 = \{0, \ldots, i-1, 15\}$
    truncate $\mathcal{L}_i$ to its first ρ_i terms
    for each $\bar{k}_i$ in $\mathcal{L}_i$ **do**
        run recursive attack on input $(\bar{k}_{15}, \bar{k}_3, \ldots, \bar{k}_{i-1}, \bar{k}_i)$
    end for
else
    for each $\bar{k}_{i_{\max}+1}, \ldots, \bar{k}_{14}$ **do**
        test key $(\bar{k}_3, \ldots, \bar{k}_{14}, \bar{k}_{15})$ and stop if correct
    end for
end if

Y_x: counter for x

R(x): rank of x

Attack on WEP

compute the ranking $\mathcal{L}_{15}$ for $I = (15)$ and $I_0 = \{0, 1, 2\}$
truncate $\mathcal{L}_{15}$ to its first ρ_{15} terms
for each $\bar{k}_{15}$ in $\mathcal{L}_{15}$ **do**
    run recursive attack on input $\bar{k}_{15}$
end for
stop: attack failed

recursive attack with input $(\bar{k}_{15}, \bar{k}_3, \ldots, \bar{k}_{i-1})$**:**

If input is only $\bar{k}_{15}$, set $i = 3$.
if $i \leq i_{\max}$ **then**
    compute the ranking $\mathcal{L}_i$ for $I = (i)$ and $I_0 = \{0, \ldots, i-1, 15\}$
    truncate $\mathcal{L}_i$ to its first ρ_i terms
    for each $\bar{k}_i$ in $\mathcal{L}_i$ **do**
        run recursive attack on input $(\bar{k}_{15}, \bar{k}_3, \ldots, \bar{k}_{i-1}, \bar{k}_i)$
    end for
else
    for each $\bar{k}_{i_{\max}+1}, \ldots, \bar{k}_{14}$ **do**
        test key $(\bar{k}_3, \ldots, \bar{k}_{14}, \bar{k}_{15})$ and stop if correct
    end for
end if

Y_x: counter for x

R(x): rank of x

The parameters are all optimized

RC4

Reminder on RC4

RC4/WEP

Tornado Attack on WEP

Challenges

RC4

Reminder on RC4

RC4/WEP

Tornado Attack on WEP

Challenges

In our EUROCRYPT'11 Paper:

We made a heuristic assumption that $V(Y_{\text{good}}) \approx V(Y_{\text{bad}})$.

In practice: $V(Y_{\text{good}}) \neq V(Y_{\text{bad}})$

We made a heuristic approximation that $(Y_{\text{good}} - Y_i)$'s are independent for all bad i's.

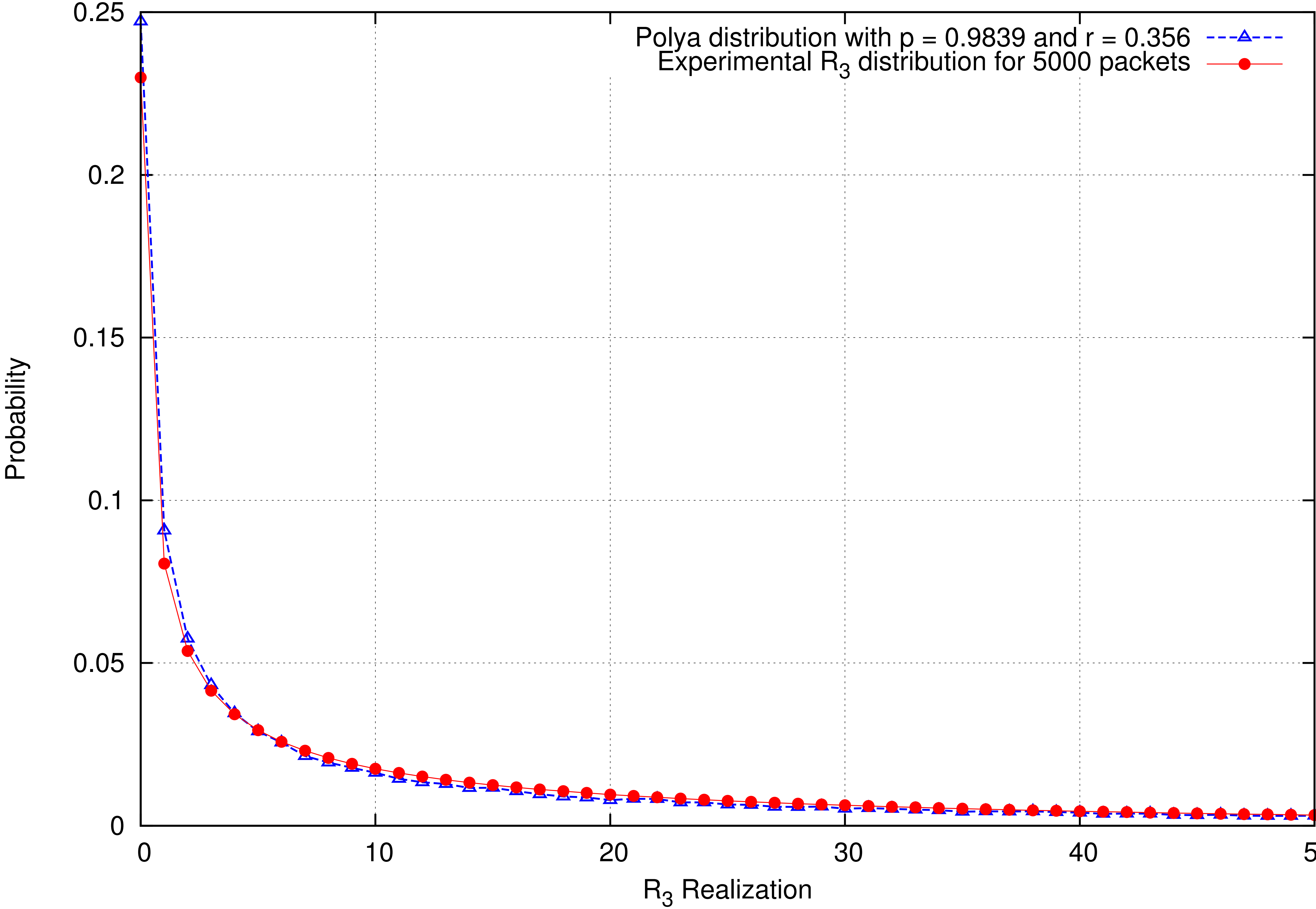
In practice: $(Y_{\text{good}} - Y_i)$'s are not independent.

Assume the rank R of the correct counter to be normally distributed.

In practice: R is not normally distributed.

Assume R is following Poisson distribution.

In practice $E(R) \neq V(R)$.



Polya distribution with p = 0.9839 and r = 0.356
Experimental R_3 distribution for 5000 packets
Probability
R_3 Realization
0.25
0.2
0.15
0.1
0.05
0
0
10
20
30
40
50

$$\Pr[X = x] = \frac{\Gamma(x+r)}{x!\,\Gamma(r)}(1-p)^r p^x$$

George Pólya
(1887-1985)

Rank of the correct counter follows the Pólya distribution.

$\Pr[R = 0] = \Pr[Y_{good} > Y_{bad(1)}, \ldots, Y_{good} > Y_{bad(255)}]$

551.578.7 : 551.577.36 : 551.501.45

(Advisory Committee on Weather Control, Washington D. C.)

The Frequency of Hail Occurrence

By

H. C. S. Thom

Summary. Hail occurrence, being a comparatively rare event, is fit well by the Poisson distribution providing the hail storms are independent. When this condition is not met, hail occurrence follows the negative binomial distribution. A test is given which determines whether the Poisson distribution may be used, or whether the negative binomial is necessary. The parameter of the Poisson distribution is always estimated efficiently by the method of moments. The parameters of the negative binomial distribution, however, are only efficiently estimated by the method of moments under certain conditions; when the method of moments fails, the method of maximum likelihood must be employed. A criterion to determine when this method must be used is given together with the method of obtaining the estimates. The methods

$$\Pr[X = x] = \frac{\Gamma(x+r)}{x!\,\Gamma(r)}(1-p)^r p^x$$

George Pólya
(1887-1985)

Rank of the correct counter follows the Pólya distribution.

$$\Pr[R = 0] = \Pr[Y_{good} > Y_{bad(1)}, \ldots, Y_{good} > Y_{bad(255)}]$$

TORNADO PROBABILITIES

H. C. S. THOM

Office of Climatology, U.S. Weather Bureau, Washington D.C.

Manuscript received July 2, 1963; revised August 7, 1963]

ABSTRACT

The frequency distributions of tornado path width and length are developed using data series from Iowa and Kansas. From these, the distribution of path area is derived. Direction of path and annual frequency are discussed. It is found that all but about 1 percent of Iowa tornadoes had path directions toward the northeast and southeast quadrants. The annual frequency for a group of Iowa counties is found to have a negative binomial distribution indicating that the climatological series is formed from a Polya stochastic process. This resembles the situation for other types of storms where the events tend to cluster. A new map of annual frequency for the United States is presented for the period 1953–62, during which it is believed tornado observation was fairly stable. The expected value of tornado area is derived from the area distribution. From this and the annual frequency, the probability of a tornado striking a point is found.

George Pólya
(1887-1985)

$$\Pr[X = x] = \frac{\Gamma(x + r)}{x!\Gamma(r)}(1 - p)^r p^x$$

Rank of the correct counter follows the Pólya distribution.

$\Pr[R = 0] = \Pr[Y_{good} > Y_{bad(1)}, \ldots , Y_{good} > Y_{bad(255)}]$

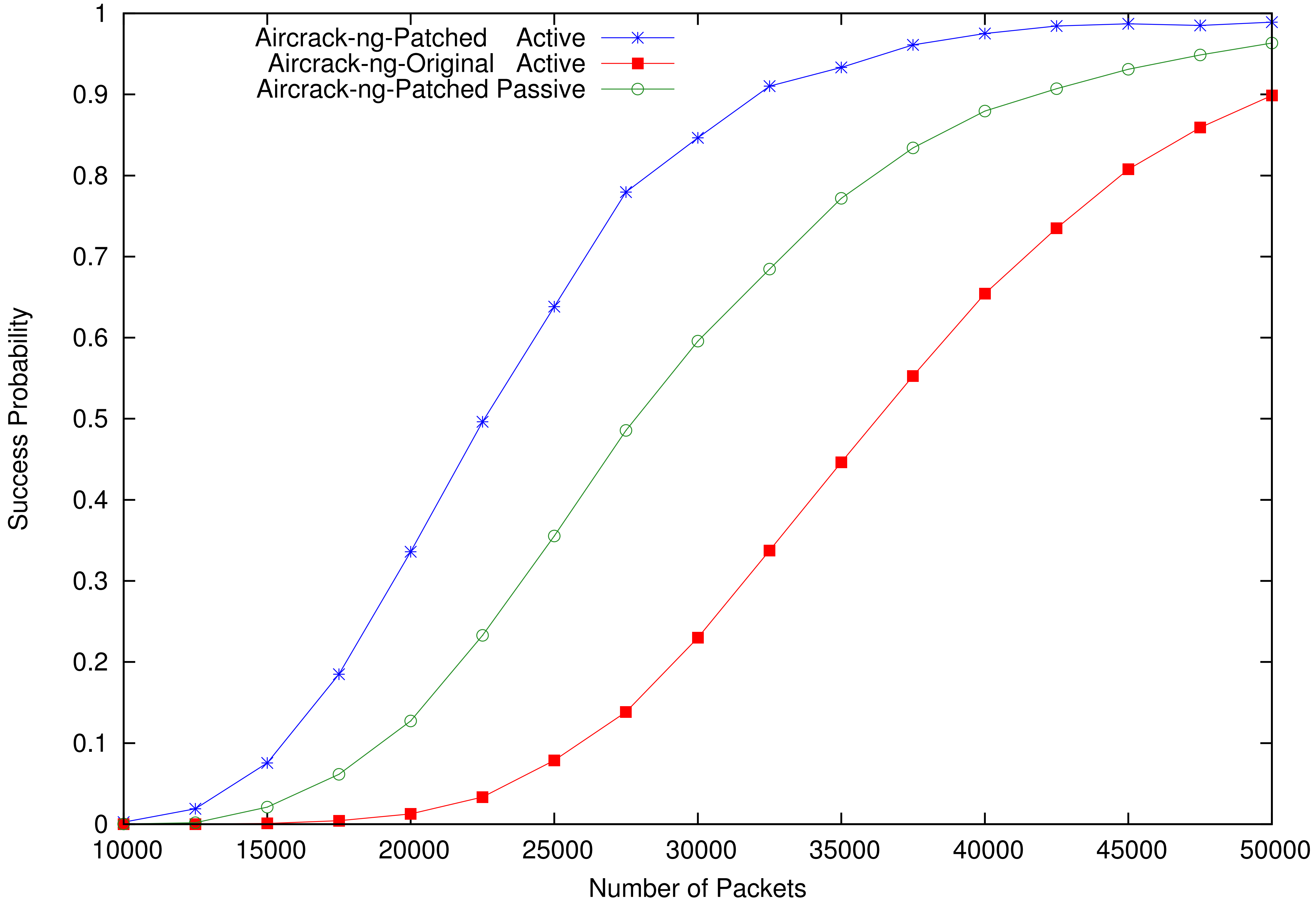
“The annual frequency for a group of Iowa counties is found to have a negative binomial distribution indicating that the climatological series is formed from a Pólya stochastic process.”

IEEE 802.11 Data Frames: Active vs. Passive Attacks

ARP Packet	
0xAA	DSAP
0xAA	SSAP
0x03	CTRL
0x00	ORG Code
0x00	
0x00	
0x08	ARP
0x06	
0x00	Ethernet
0x01	
0x08	IP
0x00	
0x06	Hardware size
0x04	Protocol
0x00	Opcode Request/Reply
0x??	
0x??	MAC addr src
0x??	
0x??	
0x??	
0x??	
0x??	
0x??	IP src
0x??	
0x??	
0x??	
0x??	MAC addr dst
0x??	
0x??	
0x??	
0x??	
0x??	

TCP/IPv4 Packet	
0xAA	DSAP
0xAA	SSAP
0x03	CTRL
0x00	ORG Code
0x00	
0x00	
0x08	IP
0x00	
0x45	IP Version + Header length
0x00	Type of Service
0x??	Packet length
0x??	
0x??	IP ID RFC815
0x??	
0x40	Fragment type and offset
0x??	
0x??	TTL
0x06	TCP type
0x??	Header checksum
0x??	
0x??	IP src
0x??	
0x??	
0x??	
0x??	IP dst
0x??	
0x??	
0x??	
0x??	Port src
0x??	
0x??	Port dst
0x??	

Comparison with Aircrack-ng



Conclusion

Conclusion

Providing the fastest attack on WEP to the date

↓

All the theory behind WEP attack with a proof

↓

Necessity of practical evaluation to ensure the correctness of theory

↓

Good understanding of the behaviour of all biases in WEP

↓

A better understanding of WPA security

Questions?