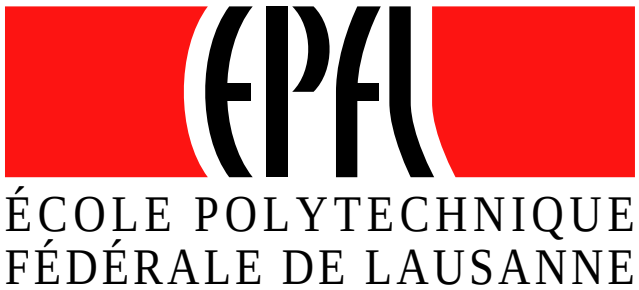
When Stream Cipher Analysis Meets Public-Key Cryptography

TCHo: A Hardware-Oriented Trapdoor Cipher

Serge Vaudenay



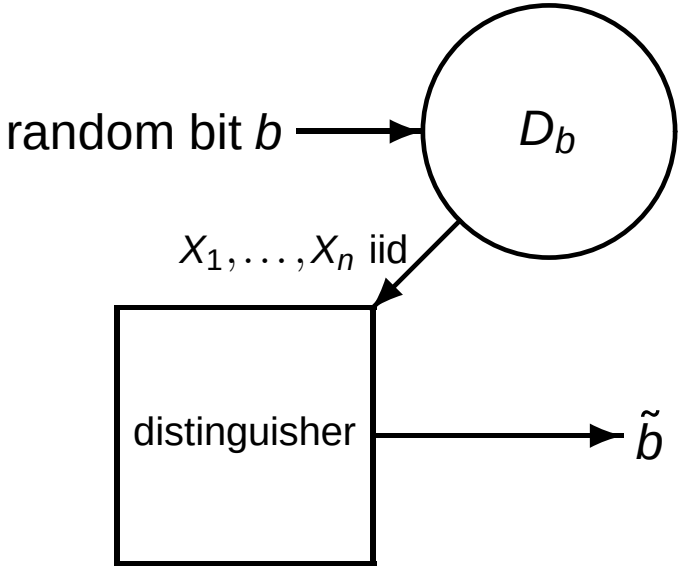
http://lasecwww.epfl.ch/

LASEC

Contribution

- Best distinguisher between random sources
  joint work with **Thomas Baignères** and **Pascal Junod**
  [BJV 2004]
- Bluetooth E0 cryptanalysis
  joint work with **Yi Lu** [LV 2004]
- TCHo1: a public-key cryptosystem
  joint work with **Matthieu Finiasz** (SAC)
- TCHo2
  joint work with **Jean-Philippe Aumasson**, **Matthieu Finiasz**, and **Willi Meier** (announcement)

Distinguishing Two Random Sources



$$\Pr[X_i = x \,|\, b] = \Pr_{D_b}[x] \qquad \text{Adv} = \Pr[b = \tilde{b}]$$

Lemma (Neyman-Pearson)

The distinguisher who outputs 1 iff $\Pr_{D_0}[X_1, \ldots, X_n] > \Pr_{D_1}[X_1, \ldots, X_n]$ *is optimal.*

When the Reference Source is Uniform

$$\Pr_{D_0}[x] = \frac{1}{Z} + \varepsilon_x \qquad \Pr_{D_1}[x] = \frac{1}{Z}$$

we assume that $\varepsilon_x \ll \frac{1}{Z}$ for any x.

$$\Pr_{D_0}[X_1, \ldots, X_n] > \Pr_{D_1}[X_1, \ldots, X_n] \iff \sum_x n_x \log(1 + Z\varepsilon_x) > 0$$

Theorem ([Baignères-Junod-Vaudenay 2004])

The best distinguisher has an advantage

$$\text{Adv} \approx 1 - 2\Phi\left(-\frac{1}{2}\sqrt{n \cdot Z \cdot \sum_x \varepsilon_x^2}\right) \text{ where } \Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt$$

so

$$\text{Adv} \approx 1 - 2\Phi\left(-\frac{1}{2}\right) \text{ for } n = \frac{1}{Z \cdot \sum_x \varepsilon_x^2}$$

SEI

$$\Pr_{D_0}[x] = \frac{1}{Z} + \varepsilon_x \qquad \Pr_{D_1}[x] = \frac{1}{Z}$$

we assume that $\varepsilon_x \ll \frac{1}{Z}$ for any x.

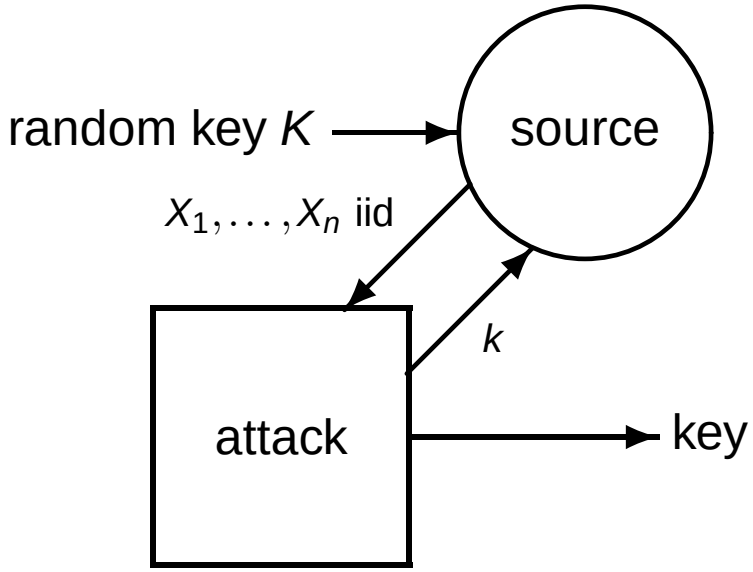
Definition (Squared Euclidean Imbalance)

$$\mathrm{SEI}(D_0) = Z \cdot \sum_x \varepsilon_x^2$$

Example: for strings of n iid bits with small bias γ, we have $\mathrm{SEI}(X) = (1+\gamma^2)^n - 1 \approx n \cdot \gamma^2$.

$\longrightarrow$ a nice toolbox that is useful for cryptanalysis

Key Recovery



$$\Pr[X_i = x | K = k] = \Pr_{D_0}[x]$$
$$\Pr[X_i = x | K \neq k] = \Pr_{D_1}[x]$$

$$\text{Adv} = \Pr[K = \text{key}]$$

Lemma (Neyman-Pearson)

The distinguisher who outputs the k of maximum likelihood ratio $\Pr_{D_0}[X_1, \ldots, X_n] / \Pr_{D_1}[X_1, \ldots, X_n]$ is optimal.

Maximum Likelihood Strategy

$$\Pr_{D_0}[x] = \frac{1}{Z} + \varepsilon_x \qquad \Pr_{D_1}[x] = \frac{1}{Z}$$

we assume that $\varepsilon_x \ll \frac{1}{Z}$ for any x.

Theorem

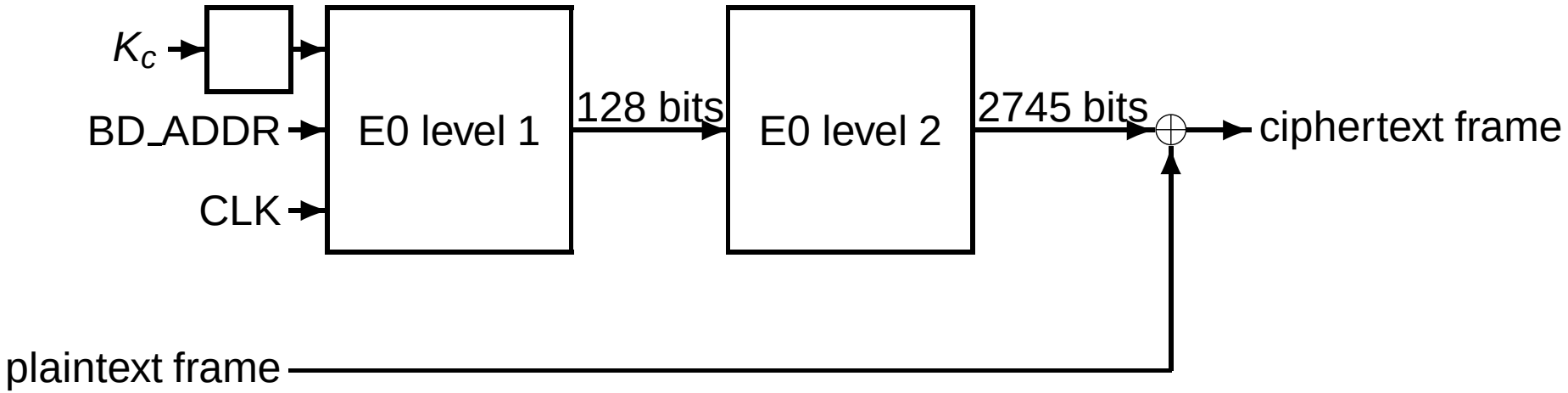
The expected rank of the right key K of L bits in the sorted list by likelihood ratio is

$$E(\text{rank}) \approx (2^L - 1) \times \Phi\left(-\sqrt{\frac{n}{2} \cdot Z \cdot \sum_x \varepsilon_x^2}\right)$$

so

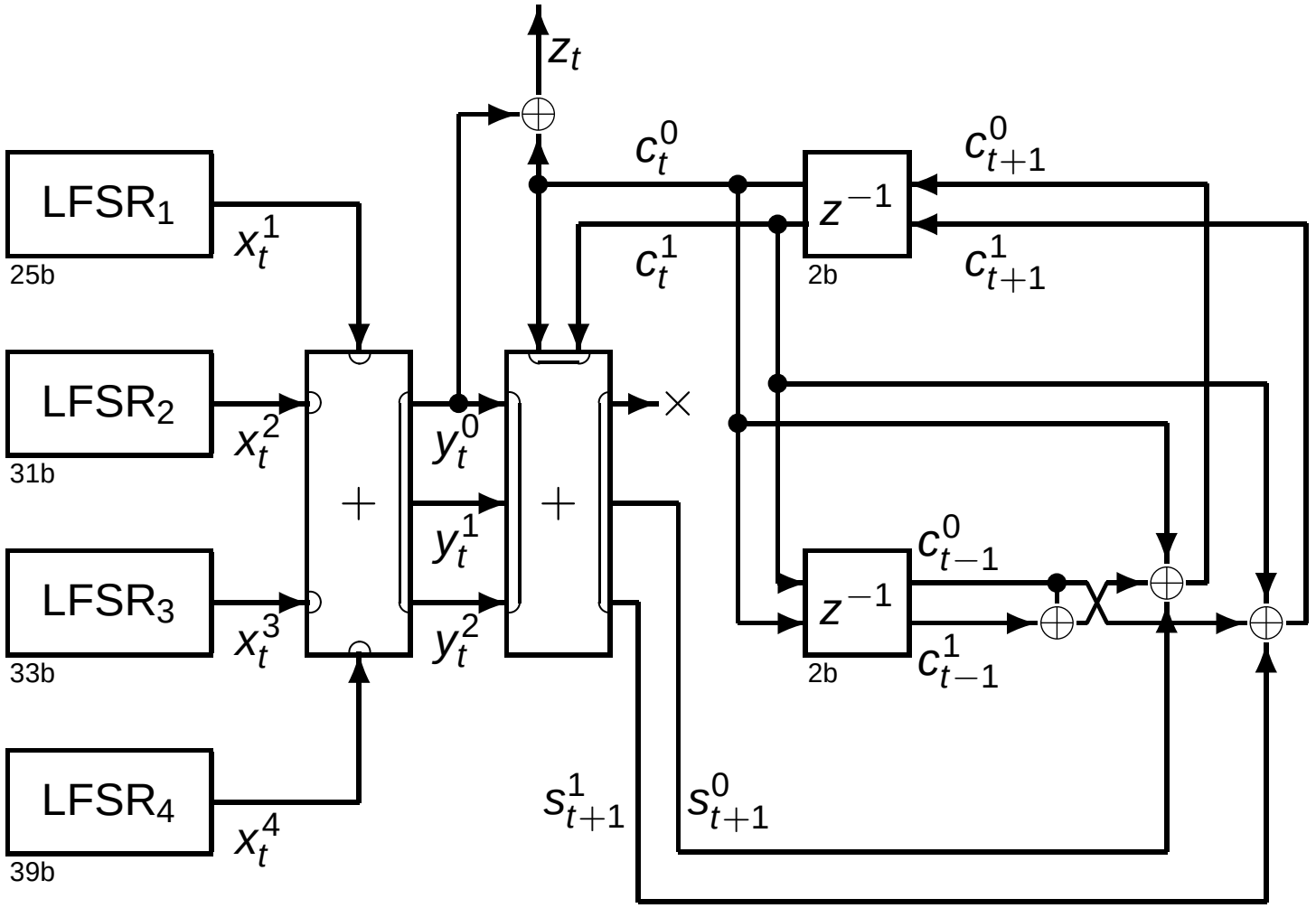
$$E(\text{rank}) \approx \frac{1}{\sqrt{2\pi}} \text{ for } n = \frac{2L \log 2}{\text{SEI}(D_0)}$$

E0 Encryption

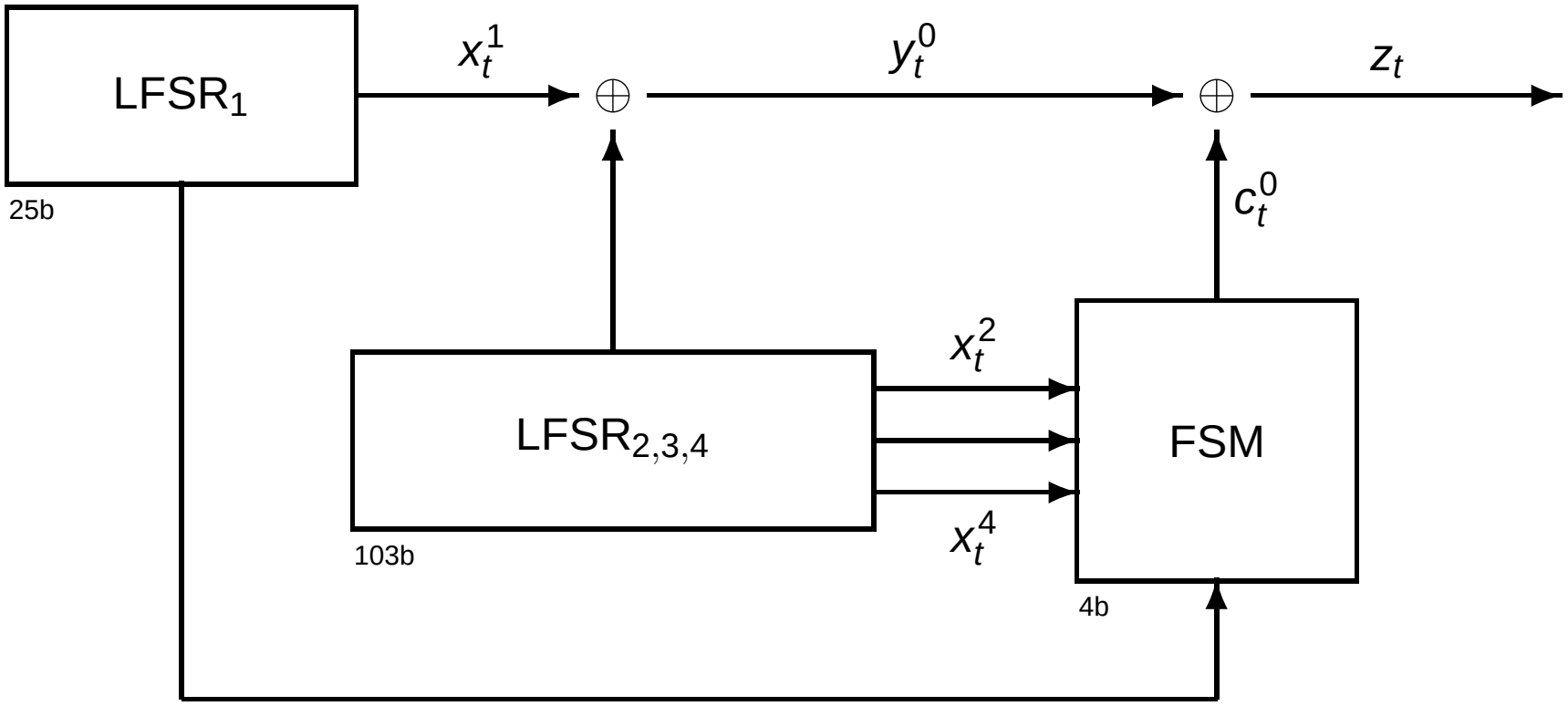


- Frames are limited to 2745 bits
- Clock-based resynchronization using an additional E0 level

One Level of E0



An Equivalent View



- Attack model: given a keystream z, get the initial state

A Technical Lemma

Notation: $\text{bias}(\text{bit}) = \Pr(\text{bit} = 0) - \Pr(\text{bit} = 1)$

Lemma ([Hermelin-Nyberg 2000])

Given $f : \mathcal{E} \times \text{GF}(2)^k \to \text{GF}(2)^k$ *and* $g : \text{GF}(2)^m \to \text{GF}(2)^k$, *let* $X \in \mathcal{E}$ *and* $Y \in \text{GF}(2)^m$ *be two independent random variables. Assuming that* $Z = g(Y)$ *is uniformly distributed in* $\text{GF}(2)^k$, *for any* $u \in \text{GF}(2)^k$ *and* $v \in \text{GF}(2)^m$, *then*

$$\text{bias}(u \cdot f(X,Z) \oplus v \cdot Y) = \sum_{w \in \text{GF}(2)^k} \text{bias}(u \cdot f(X,Z) \oplus w \cdot Z) \cdot \text{bias}(w \cdot Z \oplus v \cdot Y)$$

Application: $Y = (\sigma_1, \ldots, \sigma_t)$ is the sequence of FSM sates, $Z = \sigma_t$, and X is the next LFSR outputs to compute $f(X,Z) = \sigma_{t+1}$.

Largest Biases

Lemma

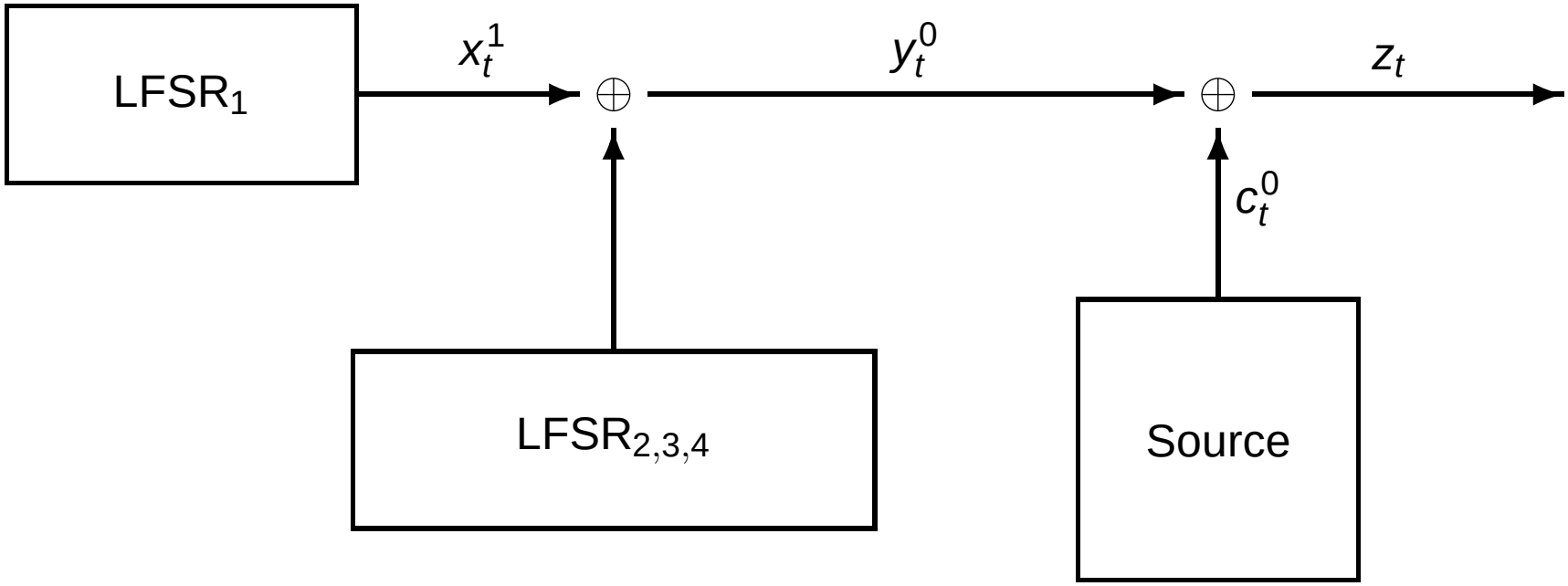
Assuming the initial state is random and uniformly distributed, we have

$$\begin{aligned} \Pr(c_t^0 \oplus c_{t+1}^0 \oplus c_{t+2}^0 \oplus c_{t+3}^0 \oplus c_{t+4}^0 = 1) &= \frac{1}{2}(1+\gamma) \\ \Pr(c_t^0 = c_{t+5}^0) &= \frac{1}{2}(1+\gamma) \end{aligned}$$

where $\gamma = \frac{25}{256}$ *is the largest possible bias.*

- These are the only two largest biases for up to 26 consecutive bits of c_t^0
- Both were already mentioned in [Ekdahl-Johansson 2000] and [Golić-Bagini-Morgari 2002]

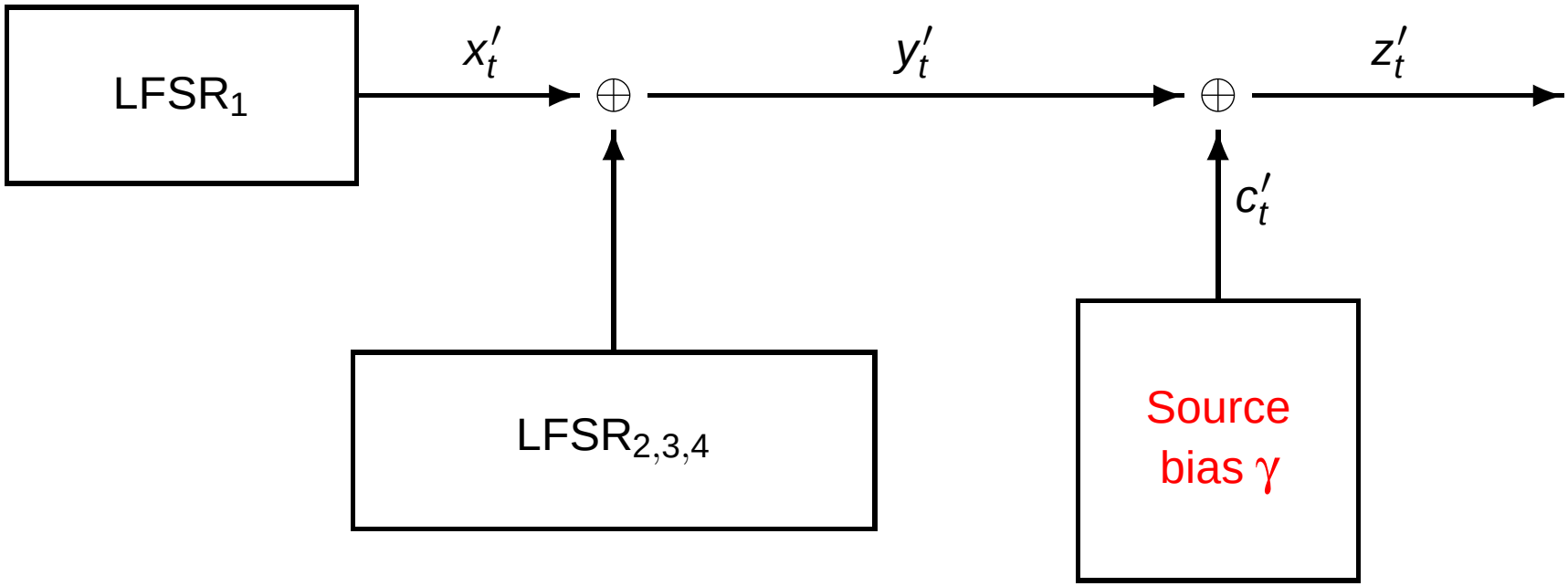
Attack Step #0: Reduce to a Biased FSM



Consider $z'_t = \alpha_1 \cdot z_{t-r+1} \oplus \cdots \oplus \alpha_r \cdot z_t$ s.t. $|\text{bias}(c'_t)| = \gamma$ is large

$$z'_t = \bigoplus_{i=1}^{r} \alpha_i \cdot z_{t-r+i} = \left(\bigoplus_{i=1}^{r} \alpha_i \cdot y^0_{t-r+i} \right) \oplus \left(\bigoplus_{i=1}^{r} \alpha_i \cdot c_{t-r+i} \right) = y'_t \oplus c'_t$$

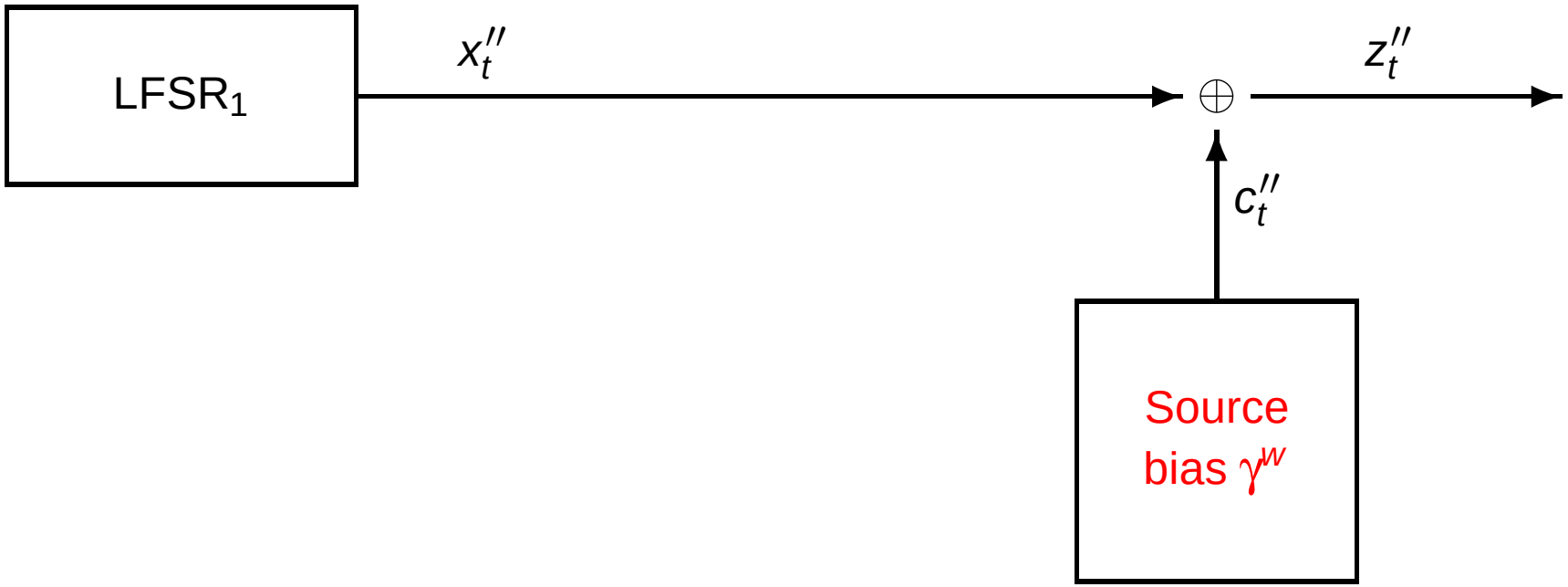
Attack Step #1: Cancel 3 LFSR out of 4



For any multiple $Q(x) = x^{q_1} + \cdots + x^{q_w}$ of the min. poly. of LFSR$_{2,3,4}$

$$z''_t = \bigoplus_{i=1}^{w} z'_{t+q_i} = \left(\bigoplus_{i=1}^{w} x'_{t+q_i} \right) \oplus \left(\bigoplus_{i=1}^{w} c'_{t+q_i} \right) = x''_t \oplus c''_t$$

Attack Step #2: Collect Statistical Information



...decoding problem: key recovery by ML decoding needs
$k \geq 2L_1\gamma^{-2w}\log 2$ bits.

$$\text{sequence } z'' = G(\text{initial LFSR}_1 \text{ state } y) \oplus \text{noise}$$

Attack Step #3: Decoding with Fast Walsh Transform

Problem: given a sequence z'' of length k and a $L_1 \times k$ generator matrix G, find the closest codeword $G(y)$

$$\mathcal{W}(x) = \sum_{t \text{ s.t. } G_t^{\perp} = x} (-1)^{z_t''}$$

We have

$$\widehat{\mathcal{W}}(y) = \sum_{x \in \mathrm{GF}(2)^L} (-1)^{y \cdot x} \mathcal{W}(x) = \sum_{t=1}^{k} (-1)^{z_t'' \oplus y \cdot G_t^{\perp}} = k - 2 \cdot \mathrm{HW}(z'' \oplus G(y))$$

	time	space
exhaustive search	$k \cdot 2^{L_1}$	k
with FWT	$k + L_1 \cdot 2^{L_1}$	$\min(k, 2^{L_1})$

$\longrightarrow$ **substantial improvement** since $k > 2^{30}$ and $L_1 = 25$ (similar trick as [Chose-Joux-Mitton 2002])

Attack Step #4: Optimization with Multi-Correlations

- using likelihood strategies: win a factor 2
- a little frustrating!
- we investigated further
- we did not find better
- with analysis based on SEI: impossible to do better

Overall Cost (Decoding the First LFSR)

(Heuristic) condition for Q to exist: $\binom{d}{w-1} \geq 2^{L_2+L_3+L_4}$

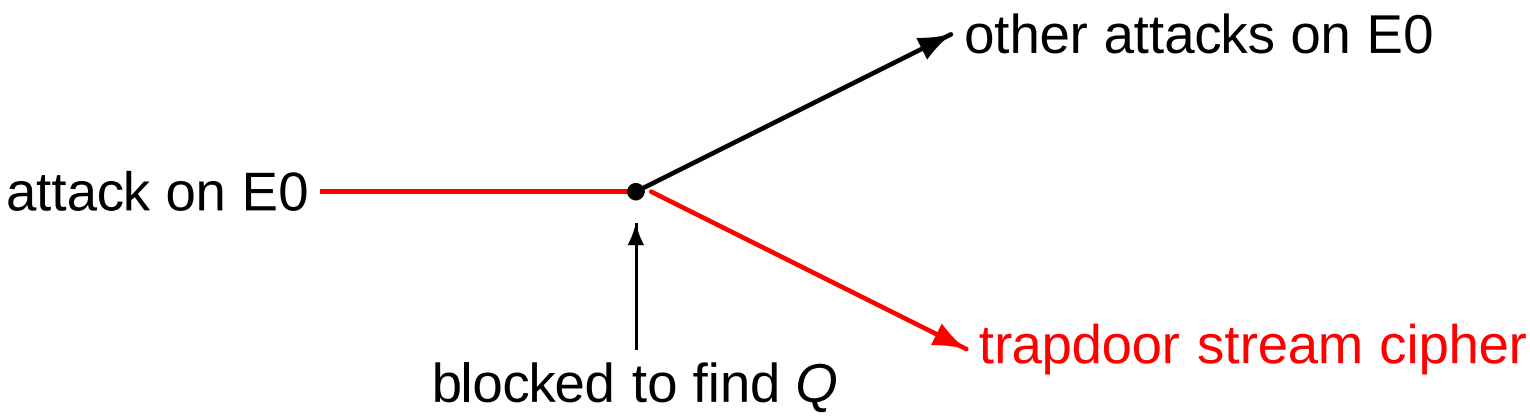
$$k = 2L_1\gamma^{-2w}\log 2 \qquad \gamma = \frac{25}{256} \qquad r = 5 \qquad L_1 = 25$$

	precomp.	time	space	data
find Q	$C_{d,w}$	-	-	-
data collection	-	$k+d+r$	k	$k+d+r$
decoding	-	$k \cdot 2^{L_1}$	$\min(k, 2^{L_1})$	-

opt without Q	-	2^{53}	2^{28}	2^{35}

($w = 4$, $d = 2^{35}$) [Lu-Vaudenay 2004]

Cryptanalysis vs Cryptography



Finding a Multiple Polynomial

Problem: find polynomial $Q(x)$, a multiple of a fixed degree-d_P polynomial $P(x)$ with degree at most d and weight at most w

for cryptanalysis

- P random
- finding one solution
- optimal for $d \approx 2^{\frac{d_P}{w-1}}$

for trapdoors

- P random factor of the solution
- finding a hidden solution
- degree $d \ll 2^{\frac{d_P}{w-1}}$

Weight 2 Case

- Let $Q(x) = 1 + x^d$ be the smallest solution.
- For $P(x)$ irreducible, its roots have order d in GF(2^{d_P}) thus d must be factor of the Mersenne number $2^{d_P} - 1$
- For $P(x)$ primitive, d must be $2^{d_P} - 1$
- General case: d must be factor of the Mersenne numbers $2^i - 1$ for any i such that there exists a factor of $P(x)$ of degree i

Weight 3: Birthday Approach

- Let $Q(x) = 1 + x^i + x^j$.
- We look for collisions $1 + x^i \bmod P(x) = x^j \bmod P(x)$:

$$\begin{pmatrix} 1+x \bmod P(x) \\ 1+x^2 \bmod P(x) \\ 1+x^3 \bmod P(x) \\ 1+x^4 \bmod P(x) \\ \vdots \\ 1+x^d \bmod P(x) \end{pmatrix} \quad = \quad \begin{pmatrix} x \bmod P(x) \\ x^2 \bmod P(x) \\ x^3 \bmod P(x) \\ x^4 \bmod P(x) \\ \vdots \\ x^d \bmod P(x) \end{pmatrix}$$

- Result:

	for cryptanalysis	**for trapdoors**
complexity	$\Theta\left(d_P \cdot 2^{\frac{d_P}{2}}\right)$	$\Theta\left(d_P \cdot d\right)$
degree	$\Theta\left(2^{\frac{d_P}{2}}\right)$	d

Odd Weight: Birthday Approach

- Let $Q(x) = 1 + x^{i_1} + \cdots + x^{i_{\frac{w-1}{2}}} + x^{j_1} + \cdots + x^{j_{\frac{w-1}{2}}}$.
- We look for collisions between the list of $(1 + x^{i_1} + \cdots + x^{i_{\frac{w-1}{2}}}) \bmod P(x)$ and $(x^{j_1} + \cdots + x^{j_{\frac{w-1}{2}}}) \bmod P(x)$.
- Result:

	for cryptanalysis	**for trapdoors**
complexity	$\Theta\left(d_P \cdot 2^{\frac{d_P}{2}}\right)$	$\Theta\left(d_P \cdot d^{\frac{w-1}{2}}\right)$
degree	$\Theta\left(2^{\frac{d_P}{w-1}}\right)$	d

Weight 5: Wagner Algorithm

- Let $Q(x) = 1 + x^i + x^j + x^k + x^\ell$.
- Wagner algorithm for $d \geq 2^{\frac{d_P}{3}}$: we look for $z_1 + z_2 + z_3 + z_4 = 0$ with $z_i \in L_i$

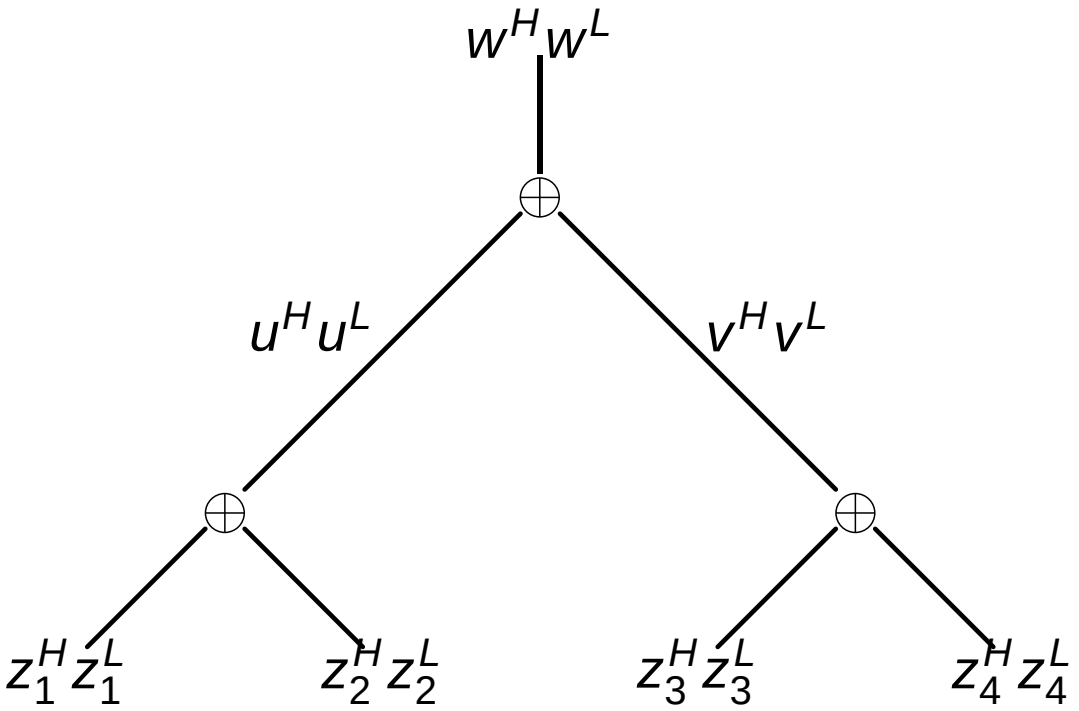
$$\underset{L_1}{\begin{pmatrix} 1+x \bmod P(x) \\ 1+x^2 \bmod P(x) \\ 1+x^3 \bmod P(x) \\ \vdots \\ 1+x^d \bmod P(x) \end{pmatrix}} \quad \underset{L_2}{\begin{pmatrix} x \bmod P(x) \\ x^2 \bmod P(x) \\ x^3 \bmod P(x) \\ \vdots \\ x^d \bmod P(x) \end{pmatrix}} \quad \underset{L_3}{\begin{pmatrix} x \bmod P(x) \\ x^2 \bmod P(x) \\ x^3 \bmod P(x) \\ \vdots \\ x^d \bmod P(x) \end{pmatrix}} \quad \underset{L_4}{\begin{pmatrix} x \bmod P(x) \\ x^2 \bmod P(x) \\ x^3 \bmod P(x) \\ \vdots \\ x^d \bmod P(x) \end{pmatrix}}$$

- Result:

	for cryptanalysis	**for trapdoors**
complexity	$\Theta\left(d_P \cdot 2^{\frac{d_P}{3}}\right)$	—
degree	$\Theta\left(2^{\frac{d_P}{3}}\right)$	—

Algorithm

Size of low parts is $\frac{d_P}{3}$, lists of $2^{\frac{d_P}{3}}$ elements



$$\left(L_1 \underset{u^L=0}{\overset{\oplus}{\bowtie}} L_2\right) \underset{w^H=0}{\overset{\oplus}{\bowtie}} \left(L_3 \underset{v^L=0}{\overset{\oplus}{\bowtie}} L_4\right)$$

Weight $2^k + 1$: Wagner Algorithm

- Result:

	for cryptanalysis	for trapdoors
complexity	$\Theta\left(w \cdot d_P \cdot 2^{\frac{d_P}{k+1}}\right)$	—
degree	$\Theta\left(2^{\frac{d_P}{k+1}}\right)$	—

- [Wagner 2002]

Syndrome Decoding

- Compute the matrix of all x^i mod $P(x)$ and do syndrome decoding.
- See [Lee-Brickell 1988], [Canteaut-Chabaud 1998]
- Result:

	for cryptanalysis	**for trapdoors**
complexity	$\Theta\left(\approx 2^{d_P}\right)$	$\Theta\left(\mathrm{Poly}(d)(d/d_P)^{w-1}\right)$
degree	$\Theta\left(2^{\frac{d_P}{w-1}}\right)$	d

Hard Instances

Assumption

When $P(x)$ is random, $w \log_2 \frac{d}{d_P} \geq c_{\text{hard}}$, and $d \leq 2^{\frac{\log_2((w-1)!)+d_P}{w-1}}$, it takes complexity $\Omega(2^{c_{\text{hard}}})$ to find any multiple of $P(x)$ of weight at most w and degree at most d.

Two generators for $P(x)$:

for cryptanalysis

- random primitive polynomial of degree d_P

for trapdoors

- factor of random polynomial of degree d and weight w until it has a primitive factor of degree $d_P \in [d_{\min}, d_{\max}]$

Reversed RSA

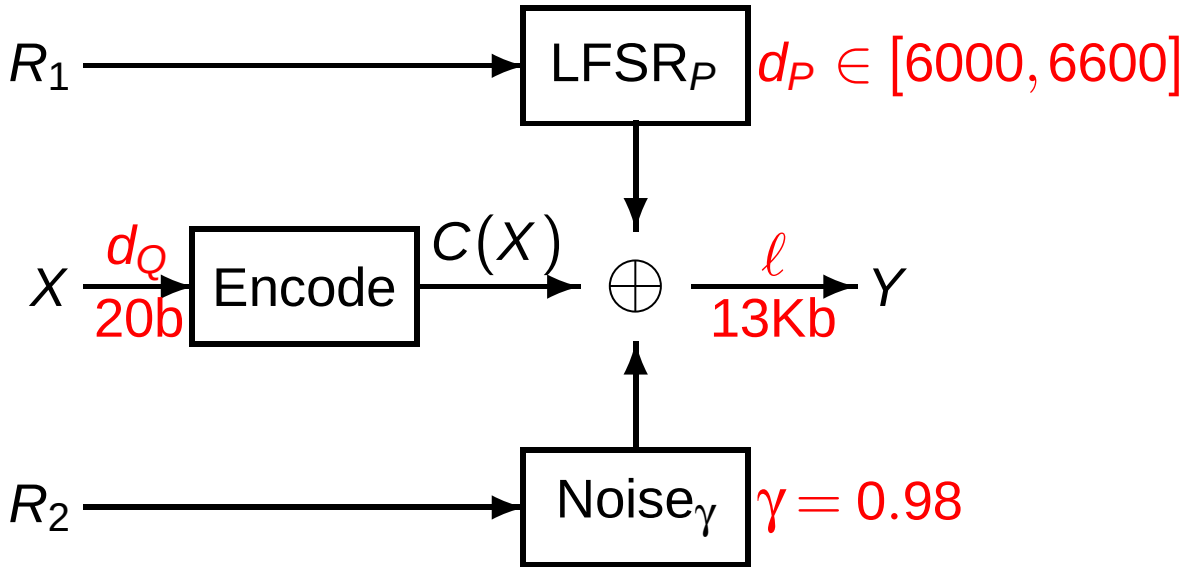
RSA

- take two prime numbers p, q
- multiply them together to n
- public key is n
- private key is p, q
- build a cryptosystem

TCHo

- take a sparse polynomial $K(x)$
- factorize it, get a factor $P(x)$
- public key is $P(x)$
- private key is $K(x)$
- build a cryptosystem

TCHo: Trapdoor Cipher, Hardware Oriented



- private key: sparse multiple of polynomial P
  $d_K = 11560$, $w_K = 99$
- well suited for hardware, can easily achieve OW-CPA security

TCHo1: LFSR-Based Code

$C(X) =$ output of LFSR seeded by X

LFSR with primitive polynomial $Q(x)$

Completeness Sufficient Conditions

Lemma

For $d_Q \leq c$ *and* $0.25 \geq \gamma^{w_K} \geq \sqrt{\frac{d_Q}{\ell - d_K} 2 \log 2}$, *by using* $K(x)$ *we can decrypt in about* 2^c *steps.*

Proof. Like in the E0 cryptanalysis:

1. "multiply" the ciphertext by $K(x)$
2. obtain a sequence of $\ell - d_K$ bits
3. do plaintext recovery by maximal likelihood strategy □

Hardness Necessary Conditions

Assumption

When $P(x)$ *is primitive and random,* $d_P \geq 2c_{\text{hard}}$, $\gamma \leq 2^{1-c_{\text{hard}}/d_P} - 1$, *and* $I \leq 1$, *decrypting a single bit of* X *takes* $\Omega(2^{c_{\text{hard}}})$ *time.*

$$I = \sum_{i=2}^{\infty} \ell \cdot C(\gamma^i) \cdot \min\left(\frac{\binom{\ell}{i}}{2^{d_P}}, \frac{2^{c_{\text{hard}}}}{\ell i}\right)$$

I: upper bound on the information we can recover within complexity $2^{c_{\text{hard}}}$ if we can use all low-weight multiples except $K(x)$.

Security

- key recovery: requires to solve the Low-Weight Multiple Problem
- message recovery: OW-CPA model

Theorem

Under the assumptions of hardness for the decryption and low-weight multiple problems, TCHo1 is $(2^{c_{\text{hard}}}, 2^{1-d_Q})$*-OW-CPA secure.*

IND-CCA Hybrid Encryption

Parallel encryption:

$$\mathrm{TCHo}^n(X_1||\cdots||X_n;R_1||\cdots||R_n) = \mathrm{TCHo}(X_1;R_1)||\cdots||\mathrm{TCHo}(X_n;R_n)$$

Fujisaki-Okamoto construction:

$$\mathrm{Enc}(X;\sigma) = \mathrm{TCHo.Enc}(\sigma;H(\sigma||X)) \;||\; \mathrm{SymEnc}_{F(\sigma)}(X)$$

Theorem (Adapted from [Fujisaki-Okamoto 1999])

If TCHo *is OW-CPA secure,* SymEnc *is FG-secure and H and F are random oracles, then* Enc *is IND-CCA secure.*

Performances

	$c_{\text{hard}} = 90$		$c_{\text{hard}} = 128$	
d_Q	20	30	20	30
d_P	$7\,000 - 7\,700$	$7\,000 - 7\,700$	$10\,000 - 11\,000$	$10\,000 - 11\,000$
γ	0.982	0.982	0.977	0.977
w_K	114	106	108	102
d_K	13 950	14 460	25 050	26 300
ℓ	15 900	16 750	29 300	31 100
ℓ_m	$\leq 2^{10}$ bits	$\leq 2^{10}$ bits	$\leq 2^{48}$ bits	$\leq 2^{48}$ bits
k	≥ 249	≥ 249	≥ 287	≥ 287
n	13	9	15	10
ℓ_σ	260	270	300	300
overhead	206 700	150 750	439 500	311 000
key gen.	$2^{36.5}$	$2^{36.5}$	$2^{38.5}$	$2^{38.5}$
key gen. time	312 s	384 s	1 362 s	1 384 s
TCHo^n encryption	2^{30}	2^{30}	2^{32}	2^{32}
encryption time	221 ms	171 ms	570 ms	400 ms
random bits	307 000	220 000	600 000	420 000
TCHo^n decryption	2^{28}	2^{38}	2^{28}	2^{38}
decryption time	11 s	–	10 s	–

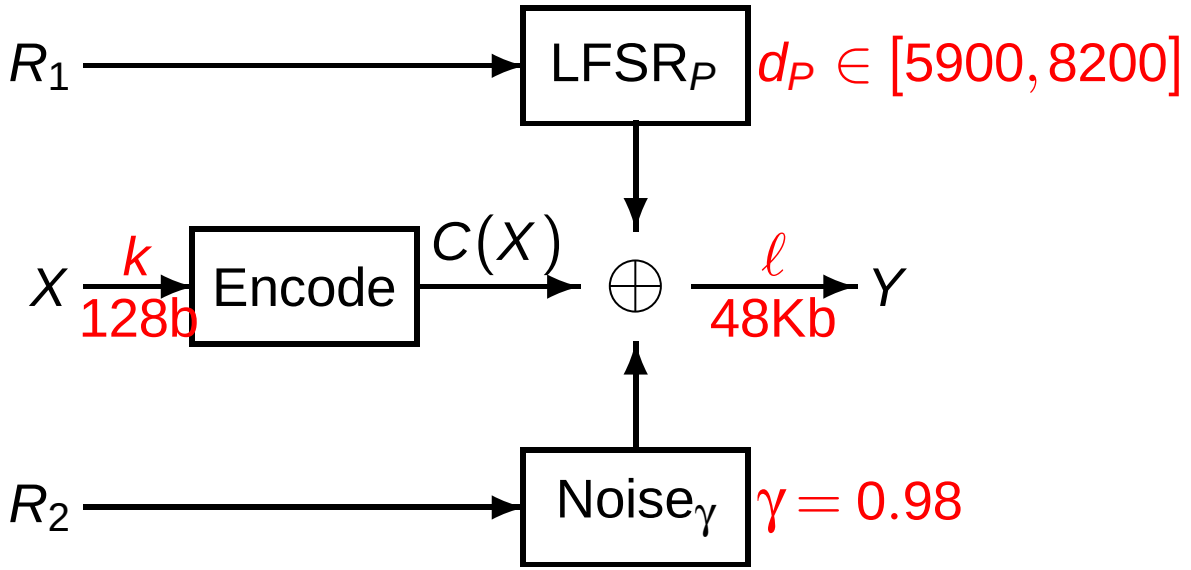
Key Idea (Thanks Willi!)

Why not using a repetition code instead of an LFSR-based one?

Results:

- decryption becomes easier than encryption
- lower expansion rate
- polynomial behavior
- IND-CPA construction

TCHo2



- private key: sparse multiple of polynomial P
  $d_K = 24420$, $w_K = 51$
- well suited for hardware, can easily achieve IND-CPA security

Complexities

RSA

- key generation: s^4
- encryption: s^2
- decryption: s^3
- best attack: $\exp\left(\left(\frac{64}{9}s\right)^{\frac{1}{3}}(\log s)^{\frac{2}{3}}\right)$
- overhead for IND-CCA security: s

TCHo2

- key generation: ℓ^2
- encryption: $\ell^{\frac{5}{3}}$
- decryption: $\ell^{\frac{4}{3}}$
- best attack: $\exp\left(\ell^{\frac{1}{3}}\right)$
- overhead for IND-CCA security: ℓ

$$w = c \quad d = c^2 k \quad \ell = \Theta(d) \quad d_{\min} = c^2 \quad d_{\max} = \Theta(c^2)$$
$$\gamma = 1 - \Theta\left(\frac{1}{c}\right) \quad k = \Theta(c)$$

Security

Theorem

Under assumptions such that the low-weight multiple polynomial problem is hard and the noisy LFSR generator is (t, ε)*-indistinguishable from a random source, TCHo is* $(t - O(\ell), \varepsilon)$*-IND-CPA secure.*

The Noisy LFSR Distinguishability Problem

Assumption

If $d_{\min} \geq 2c$ *and* $\gamma \leq 2^{1-c/d_{\min}} - 1$ *and if the conditions of LWMP Assumption are met then, a distinguisher between* $\mathcal{S}^{\ell}_{\mathcal{L}_P} + \mathcal{S}^{\ell}_{\gamma}$ *and* $\mathcal{S}^{\ell}_{0}$ *has an advantage/complexity ratio lower than*

$$R = \max_{\substack{v \in [0, d_{\max}] \\ N \geq 1}} \frac{\gamma^v / \sqrt{2\pi}}{v\sqrt{N} + \frac{1}{\sqrt{N}} \left(\frac{\ell}{d_{\min}} \right)^{v-1} \times \frac{2^{d_{\min}}}{\binom{\ell}{v}}}$$

Hint

- collect biased bits by collecting multiples of P of weight v and degree $\leq \ell$
- number of bits of bias γ^v: $N_v \approx 2^{-d_P} \binom{\ell}{v}$
- number of used bits to attack: $N \leq N_v$
- complexity to recover those bits: $\geq vN + (\ell/d_P)^{v-1} \times 2^{d_P} / \binom{\ell}{v-1}$
- best advantage using those bits: $\text{Adv} \approx \gamma^v \sqrt{N/(2\pi)}$
- best advantage/complexity ratio:

$$R = \max_{\substack{v \in [0, d_P] \\ N \geq 1}} \frac{\gamma^v / \sqrt{2\pi}}{v\sqrt{N} + \frac{1}{\sqrt{N}} \left(\frac{\ell}{d_P}\right)^{v-1} \times \frac{2^{d_P}}{\binom{\ell}{v}}}$$

(maximum is typically reached for $N = 1$)

Vectors of Parameters

	k	d_P	d_K	w_K	γ	$\frac{1}{2}(1-\gamma^w)$	ℓ	ρ
I_{65}	128	$\in [5\,800, 7\,000]$	25 820	45	0.9810	0.29	50 000	$2^{-26.7}$
II_{65}	128	$\in [8\,500, 12\,470]$	24 730	67	0.987	0.292	68 000	$2^{-48.5}$
III	128	$\in [3\,010, 4\,433]$	44 677	25	$1-\frac{3}{64}$	0.349	90 000	$2^{-22.4}$
IV	128	$\in [7\,150, 8\,000]$	24 500	51	0.98	0.322	56 000	$2^{-22.9}$
V	128	$\in [6\,000, 8\,795]$	17 600	81	$1-\frac{3}{128}$	0.427	150 000	$2^{-13.0}$
VI	128	$\in [9\,000, 13\,200]$	31 500	65	$1-\frac{1}{64}$	0.320	100 000	$2^{-54.7}$

Vectors of Parameters

	encryption	decryption	key gen.	unreliability	private key	public key	plaintext	ciphertext
I_{65}	55 ms	70 ms	682 s	$2^{-26.7}$	660 b	7 000 b	128 b	50 000 b
II_{65}	148.0 ms	115.4 ms	467 s	$2^{-48.5}$	507 b	12 470 b	128 b	68 000 b
III	75.5 ms	49.0 ms	2 560 s	$2^{-22.4}$	281 b	4 433 b	128 b	90 000 b
IV	90.1 ms	65.1 ms	650 s	$2^{-22.9}$	506 b	8 000 b	128 b	56 000 b
V	228.4 ms	423.7 ms	261 s	$2^{-13.0}$	726 b	8 795 b	128 b	150 000 b
VI	232.5 ms	178.7 ms	614 s	$2^{-54.7}$	652 b	13 200 b	128 b	100 000 b

(include: PRG ISAAC [Jenkins 1996])

Hardware: $\sim$10000 gates, 4MHz, 15ms to encrypt, overhead of 50Kb.

IND-CCA Hybrid Encryption

- KEM/DEM construction + IND-P2-C2 symmetric encryption

$$\mathrm{Enc}(X;\sigma||r) = \mathrm{TCHo.Enc}(\sigma;r) \;||\; \mathrm{SymEnc}_{F(\sigma)}(X)$$

[Cramer-Shoup 2004], [Dent 2002]

- tag-KEM/DEM Fujisaki-Okamoto revisited construction

$$\begin{array}{c} y \\ \shortparallel \\ \mathrm{Enc}(X;\sigma) = \mathrm{TCHo.Enc}(\sigma;H(\sigma||y)) \;||\; X + F(\sigma) \end{array}$$

[Abe-Gennaro-Kurosawa 2005],
[Abe-Gennaro-Kurosawa-Shoup 2005]

Conclusion

- Stream cipher cryptanalysis provides new insights for making new cryptosystems
- Low-Weight Multiple Problem:
  a combinatorial problem for post-quantum cryptography?
- TCHo: strong encryption for tiny hardware
- please break us!
- TCHo: a Win-win cryptographic construction
  - either we get a secure cryptosystem
  - or we get new algorithms for breaking stream ciphers

References

- Abe-Gennaro-Kurosawa 2005: IACR ePrint 2005/027
- Abe-Gennaro-Kurosawa-Shoup 2005: EUROCRYPT 2005
- Baignères-Junod-Vaudenay 2004: ASIACRYPT 2004
- Canteaut-Chabaud 1998: IEEE Transactions on Information Theory vol. 44
- Chose-Joux-Mitton 2002: EUROCRYPT 2002
- Cramer-Shoup 2004: SIAM Journal of Computing vol. 33
- Dent 2002: IACR ePrint 2002/174
- Ekdahl-Johansson 2000: Joint Conference on Communications and Coding 2000
- Fujisaki-Okamoto 1999: CRYPTO 1999
- Golić-Bagini-Morgari 2002: EUROCRYPT 2002
- Hermelin-Nyberg 2000: ICISC 1999
- Jenkins 1996: FSE 1996
- Lee-Brickell 1988: EUROCRYPT 1988
- Lu-Vaudenay 2004: CRYPTO 2004
- Wagner 2002: CRYPTO 2002