Cryptanalysis of Bluetooth Keystream Generator Two-level E0

Yi LU and Serge VAUDENAY

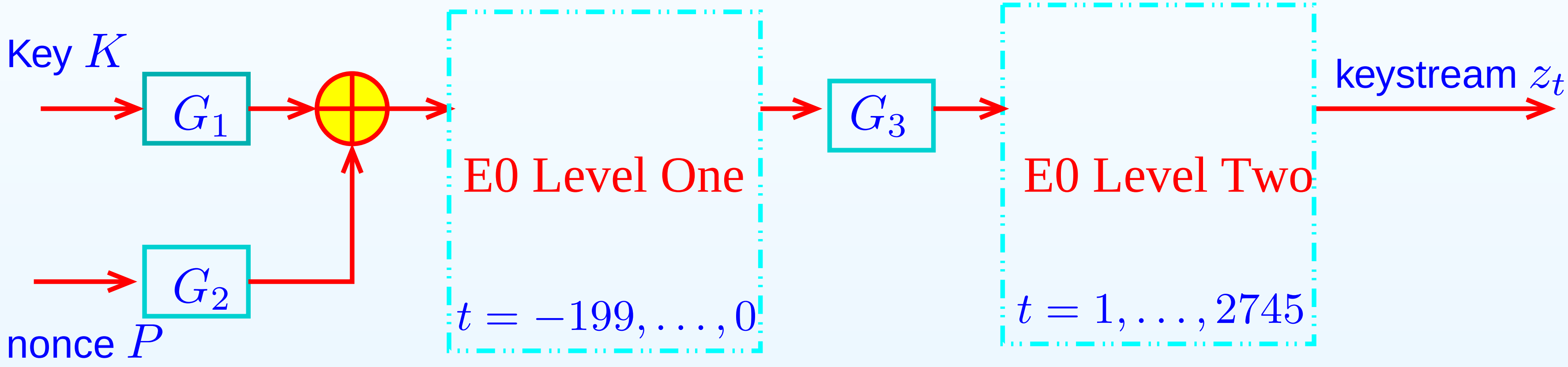
`http://lasecwww.epfl.ch`

EPFL

Outline

- Review on Bluetooth Two-level E0
- One Resynchronization Flaw
- First Attacks
- Extended Key-recovery Attack
- Conclusion

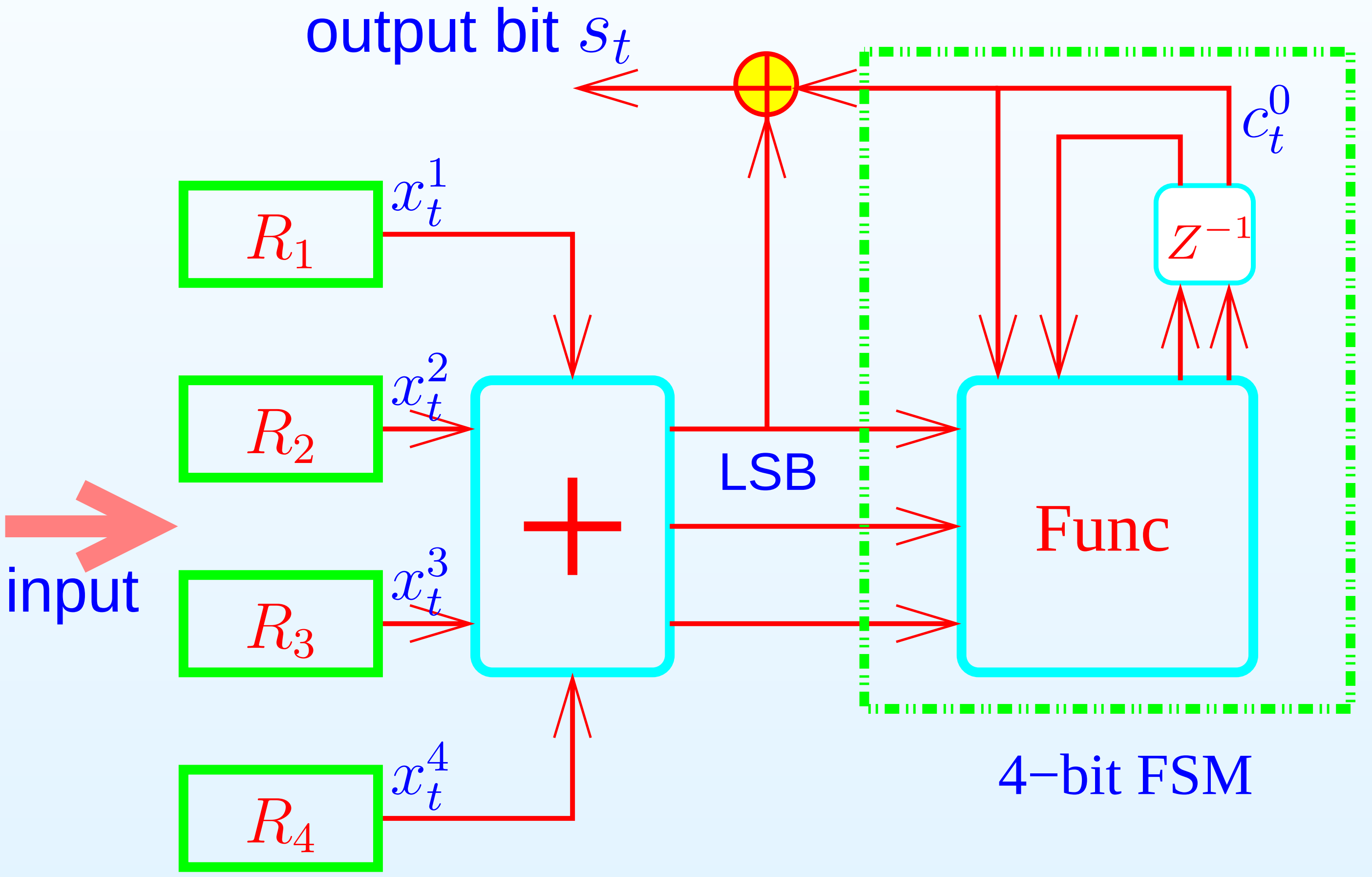
Review on Bluetooth Two-level E0



G_1, G_2, G_3: affine transformations

The Core of Bluetooth E0

$$s_t = x_t^1 \oplus x_t^2 \oplus x_t^3 \oplus x_t^4 \oplus c_t^0.$$



The Core of Bluetooth E0 (Cont'd)

- The bit length L_i of each R_i is:

$$\left.\begin{array}{rcl} L_1 & = & 25 \\ L_2 & = & 31 \\ L_3 & = & 33 \\ L_4 & = & 39 \end{array}\right\} \Longrightarrow \sum_i L_i = 128.$$

- Statistical properties of $\{c_t^0\}$ were well-studied by Lu-Vaudenay'04 based on previous work of Hermelin-Nyberg'99, Ekdahl-Johansson'00, Golić et al.'02.

The Core of Bluetooth E0 (Cont'd)

The two largest biases up to 26 consecutive bit $\{c_t^0\}$ are:

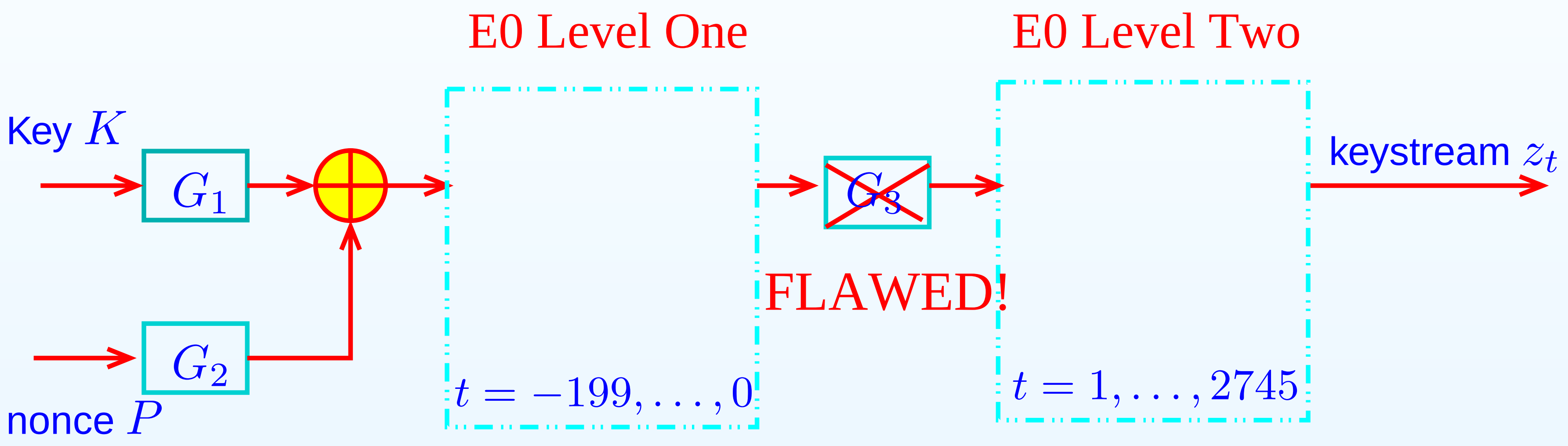
$$\begin{aligned}
\Pr(c_t^0 \oplus c_{t+1}^0 \oplus c_{t+2}^0 \oplus c_{t+3}^0 \oplus c_{t+4}^0 = 1) &= \frac{1}{2} + \frac{\lambda}{2}, \\
\Pr(c_t^0 \oplus c_{t+5}^0 = 0) &= \frac{1}{2} + \frac{\lambda}{2},
\end{aligned}$$

where $\lambda = \frac{25}{256}$.

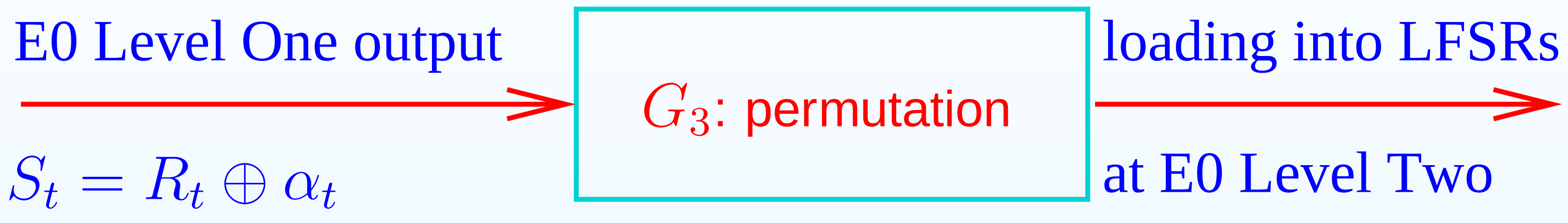
Content

- Review on Bluetooth Two-level E0
- One Resynchronization Flaw
- First Attacks
- Extended Key-recovery Attack
- Conclusion

One Resynchronization Flaw



Resynchronization Flaw: Closer Look at G_3



where

- $R = (M \circ G_1)(K) \oplus (M \circ G_2)(P)$,
- α_t's = $\{c_t^0\}$ produced by E0 level One.

Effect of Permutation G_3

The first 24 output bits of LFSRs at Level Two are:

R_1	$S_{-127}, \ldots, S_{-120}$	$S_{-95}, \ldots, S_{-88}$	$S_{-63}, \ldots, S_{-56}$
R_2	$S_{-119}, \ldots, S_{-112}$	$S_{-87}, \ldots, S_{-80}$	$S_{-55}, \ldots, S_{-48}$
R_3	$S_{-79}, \ldots, S_{-72}$	$S_{-47}, \ldots, S_{-40}$	$S_{-23}, \ldots, S_{-16}$
R_4	$S_{-71}, \ldots, S_{-64}$	$S_{-39}, \ldots, S_{-32}$	$S_{-15}, \ldots, S_{-8}$

where $S_t = R_t \oplus \alpha_t$ denotes output of E0 Level One.

Correlation of Bluetooth Two-level E0

Let

- $U = G_3 \circ R = (G_3 \circ M \circ G_1)(K) \oplus (G_3 \circ M \circ G_2)(P)$.
- β_t's = $\{c_t^0\}$ produced by E0 level Two.

THEOREM. Assuming independence of α_t's and β_t's, within one frame, we have

$$\Pr\left(\bigoplus_{j=0}^{4}(z_{t+j} \oplus U_{t+j}) = 1\right) = \frac{1}{2} + \frac{\lambda^5}{2},$$

for $t \in \{1, \ldots, 4\} \cup \{9, \ldots, 12\} \cup \{17, \ldots, 20\}$.

Content

- Review on Bluetooth Two-level E0
- One Resynchronization Flaw
- First Attacks
- Extended Key-recovery Attack
- Conclusion

First Attacks on Two-level E0: Distinguishing Attack

By linear cryptanalysis, we expect that with $\lambda^{-10} \approx 2^{34}$ samples,

$$\bigoplus_{j=0}^{4} (z_{t+j} \oplus U_{t+j}) = 1$$

holds for $t \in \{1, \ldots, 4\} \cup \{9, \ldots, 12\} \cup \{17, \ldots, 20\}$ most of the time.

As $U^i \oplus U^j = (G_3 \circ M \circ G_2)(P^i \oplus P^j)$ is known, we can recover one bit $\oplus_{j=0}^{4} U^1_{1+j}$ separately with two sets of 2^{34} frames and expect a unique solution.

One Easy Decoding Problem

Given L-bit sequences $s^1, \ldots, s^m$ and $\delta^1, \ldots, \delta^m$, such that $\delta^1 = \mathbf{0}$ and $\delta^i \neq \delta^j$ for all $i \neq j$, find the L-bit sequence r^1 that maximizes

$$N(r^1) = \sum_{i=1}^{m} \sum_{t=1}^{L} (s_t^i \oplus r_t^i),$$

where $r_t^i = r_t^1 \oplus \delta_t^i$ for $i = 1, \ldots, m$ and $t = 1, \ldots, L$.

Solution:

$$r_t^1 = \text{minority}\{s_t^i \oplus \delta_t^i : i = 1, \ldots, m\}$$

for all $t = 1, \ldots, L$.

Distinguishing Attack Complexities

Type	Frames	Data and Time
basic	2^{35}	2^{37}
improved	2^{33}	2^{36}

First Attacks on Two-level E0: Key-recovery Attack

- Fixing $t \in \{1, \ldots, 4\} \cup \{9, \ldots, 12\} \cup \{17, \ldots, 20\}$, we independently recover twelve key bits by previous method.
- Then, we try exhaustively for the remaining key bits.

Let $|\mathcal{K}|$ be the effective key length.

Frames	Data	Time	Memory
2^{34}	$2^{38.6}$	$2^{34} + 2^{\|\mathcal{K}\|-13}$	2^{34}

Note that this is the first non-trivial attack on two-level E0 with variable key length.

Content

- Review on Bluetooth Two-level E0
- One Resynchronization Flaw
- First Attacks
- Extended Key-recovery Attack
- Conclusion

Extended Attack: Main Idea

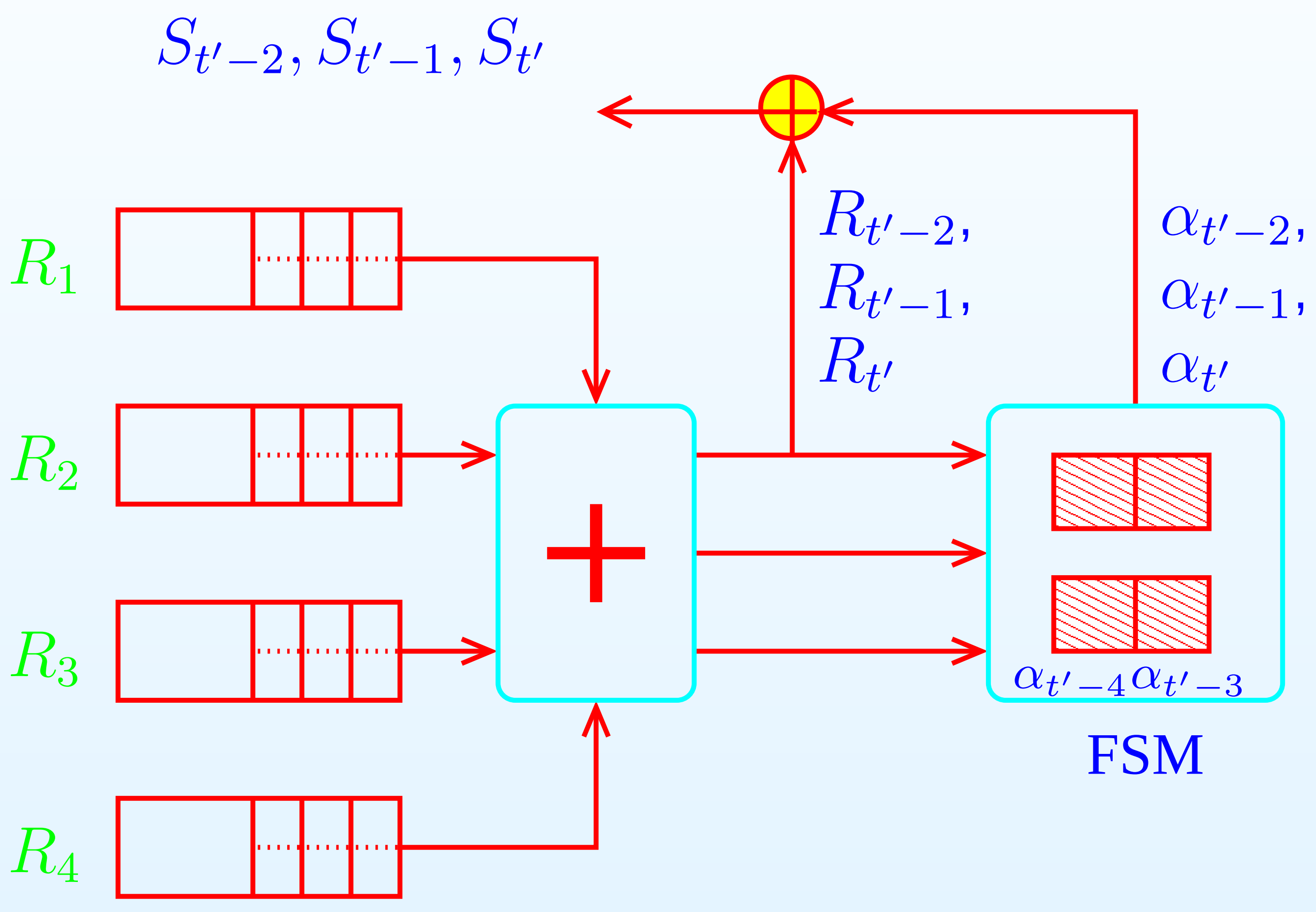
Recall that

$$\bigoplus_{j=0}^{4} (z_{t+j} \oplus U_{t+j})$$

corresponds to XOR of five i.i.d. biased bits.

$\Longrightarrow$ Try to cancel one biased bit for all frames by exhaustive search!

Partial Key-recovery Attack



Partial Key-recovery Attack: Main Algorithm

Let $f : \{0,1\} \to \mathbf{R}$ to be determined later.

fix t'
for all 12-bit $\mathcal{K}$ **do**
  initialize counters to zero μ_0, μ_1
  for each frame i **do**
    for all 4-bit FSM state σ at time $t' - 3$ **do**
      compute $\alpha_{t'-2}, \alpha_{t'-1}, \alpha_{t'}$
      $b \Longleftarrow \bigoplus_{j=0}^{4} (z_{t+j} \oplus U_{t+j}) \oplus \bigoplus_{j=0}^{4} \alpha_{t'-j}$
      increment μ_b
    end for
  end for
  $G_{\mathcal{K}} = \sum_b \mu_b f(b)$
end for
output $\mathcal{K}$ with the largest $G_{\mathcal{K}}$

Partial Key-recovery Attack: (Cont'd)

Since we know

$$\text{bias}(b) = \begin{cases} \lambda^4, & \text{right } \mathcal{K} \text{ and right } \sigma \\ \lambda^6 \approx 0, & \text{otherwise.} \end{cases}$$

Using theory of Baignères, Junod and Vaudenay'04, data complexity is minimized when we choose

$$f = \frac{D_1 + 15D_0}{16},$$

where

- D_0: uniform distribution,
- D_1: distribution with bias λ^4.

The Overall Key-recovery Attack: Complexities

Attack	PreComp.	Time	Frames	Data	Space
Fluhrer-Lucks'01	-	2^{73}	-	2^{43}	2^{51}
Fluhrer'02	2^{80}	2^{65}	2	$2^{12.4}$	2^{80}
Golić et al.'02	2^{80}	2^{70}	45	2^{17}	2^{80}
Our Attack	-	2^{40}	2^{35}	$2^{39.6}$	2^{35}

Conclusion

- One resynchronization flaw of Bluetooth two-level E0 was studied.
- Based on the flaw, we propose the short-cut attacks on Bluetooth two-level E0, which doesn't recover the key level by level.
- Considering the fact that the maximum number of available frames is 2^{26}, our attacks still remain academic interest.
- Our attack illustrates theory of statistical attacks by Baignères, Junod and Vaudenay'04.