Attacks against TSC

Simon Künzli, Pascal Junod*, Willi Meier

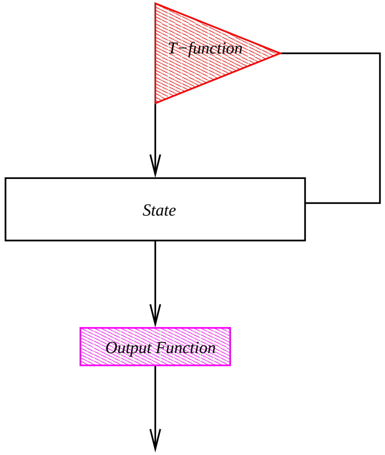
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Fachhochschule Aargau
Nordwestschweiz
University of Applied Sciences

Paris (France), February 21$^{\text{st}}$, 2005

TSC Stream Ciphers

- TSC-1 / TSC-2: proposed by Hong, Lee, Yeom, and Han at FSE'05 / SASC'04
- Structure:



More precisely...

$$\boldsymbol{x}^t = \begin{pmatrix} 1 & 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & 1 & \cdots & 0 & 1 \\ 1 & 1 & 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix}$$

- State $\boldsymbol{x}^{\boldsymbol{t}}$ updated by an *odd parameter* $\alpha(.)$ (which is a kind of T-function).
- $\alpha(\boldsymbol{x}) = (p + \mathtt{C}) \oplus p \oplus 2s$ where $\mathtt{C} = \mathtt{0x12488421}$, $p = x_0 \wedge x_1 \wedge x_2 \wedge x_3$, and $s = x_0 + x_1 + x_2 + x_3$.
- If $[\alpha^t]_i = 0$, then $[\boldsymbol{x}^{t+1}]_i \leftarrow \text{sbox}\left(\text{sbox}\left([\boldsymbol{x}^t]_i\right)\right)$.
- Otherwise, $[\boldsymbol{x}^{t+1}]_i \leftarrow \text{sbox}\left([x^t]_i\right)$
- Output function: $f(\boldsymbol{x}) = (x_{0 \lll 9} + x_1)_{\lll 15} + (x_{s \lll 7} + x_3)$.

S-box

$$\text{sbox}(a) = \{3, 5, 9, 13, 1, 6, 11, 15, 4, 0, 8, 14, 10, 7, 2, 12\}$$

- Single cycle S-box: $\text{sbox}^{16}(a) = a$
- Designed such that $\forall i, \Pr\left[[a \oplus \text{sbox}(a)]_i = 0\right] = \Pr\left[[a \oplus \text{sbox}^2(a)]_i = 0\right] = \frac{1}{2}$
- But: we observed that for $\delta \equiv 0 \pmod 4$, $\forall i, \Pr\left[[a \oplus \text{sbox}^\delta(a)]_i = 0\right] = \frac{1}{2} + \varepsilon$ with $|\varepsilon| \gg 0$.

Back to the State

- We know that the event defined by $X_\delta = 1$ iff $[a]_i = \mathsf{sbox}^\delta([a]_i)$ is biased for some δ's.
- Idea: look for (biased) events defined by $Y_\Delta = 1$ iff $[\boldsymbol{x}_j^t]_i = [\boldsymbol{x}_j^{t+\Delta}]_i$.
- We observed that $\Pr[Y_{11} = 1] \approx 0.6007$ and that $\Pr[Y_8 = 1] \approx 0.4004$
- Due to the specific output function: repeating bits in the state result in repeating bits in the keystream (for instance $\mathsf{lsb}(\boldsymbol{y}^t \oplus \boldsymbol{y}^{t+8})$).
- Data complexity: 2^{22} words of keystream required to distinguish it from a perfect random sequence.

Another Attack Independent of the S-box Structure

- Think about a perfect (but non-existing) single-cycle S-box, i.e., perfectly balanced for all $\delta < 16$.
- In that case, we are still able exploit the event that the S-box was applied 16 times.
- Going through the output function is more complicated but doable.

TSC-2

- $\alpha(.)$: instead of two applications of the S-box, one applies the *identity mapping*.
- Small size of $\alpha(.)$: 32-bit state drives the behaviour of a 128-bit state. This is a problem.
- We have to wait until a "nice" output of $\alpha(.)$ occurs and to exploit it.

Thank You!