Indian Statistical Institute
KOLKATA

A Differential Fault Attack on MICKEY 2.0

Subhadeep Banik and Subhamoy Maitra

Presented by Meltem Sönmez Turan

CHES 2013
UCSB, Santa Barbara

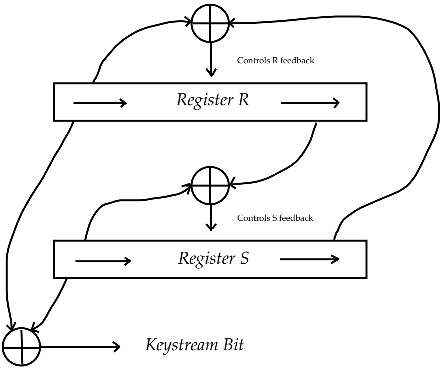
Outline

- Description of the stream cipher Mickey 2.0
- Recovering internal state given partial inputs
- Differential fault attack with chosen-location faults
- Differential fault attack with random-location faults

MICKEY 2.0

- Proposed by Steve Babbage and Matthew Dodd in 2004
- Part of eSTREAM's hardware portfolio
- Bit-oriented, Synchronous stream cipher
- The first version (1.0) of the cipher was cryptanalyzed
  1. A TMD-Tradeoff Attack by Hong et al. (INDOCRYPT 2005)
  2. Uses low Sampling Resistance of the cipher.
- Response $\Rightarrow$ Increase State size from 160 to 200.

Generic Structure



- The registers R, S are 100 bits long.
- Each exercises Mutual Control over the other.

Initialization of Cipher

- Supports an 80 bit Key and a v-bit IV $(0 \leq v \leq 80)$
- The regs R, S are both initialized with all $0's$.

1	IV Loading	**for** $i = 0$ to $v - 1$ CLOCK_KG $(R, S, 1, iv_i)$
2	Key Loading	**for** $i = 0$ to 79 CLOCK_KG $(R, S, 1, k_i)$
3	Pre Clock	**for** $i = 0$ to 99 CLOCK_KG $(R, S, 1, 0)$
4	PRGA	**while required** $z = r_0 + s_0$ CLOCK_KG $(R, S, 0, 0)$

A Few Observations

- Let $a_0, a_1, a_2, a_3 \in \mathrm{GF}(2)$. Let a_0 be defined as follows

$$a_0 = \begin{cases} a_2, & \text{if } a_1 = 0 \\ a_3, & \text{if } a_1 = 1. \end{cases}$$

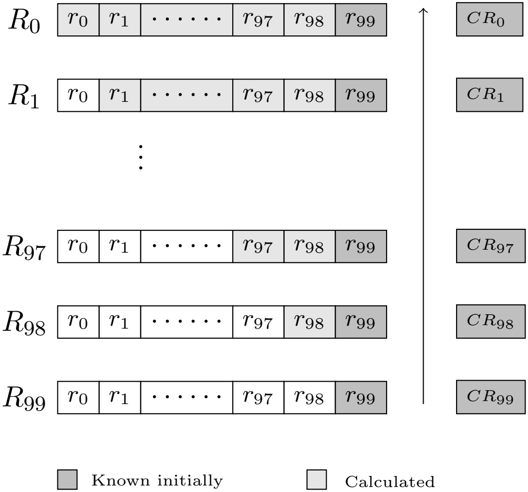
- Then it is straightforward to see that a_0 can be expressed as a multivariate polynomial over GF(2), i.e., $a_0 = (1 + a_1) \cdot a_2 + a_1 \cdot a_3$.

- MICKEY uses a lot of If-Else constructs in its State Update. $\rightarrow$ So the state update may be equivalently expressed as a series of multi-variate polynomials over GF(2).

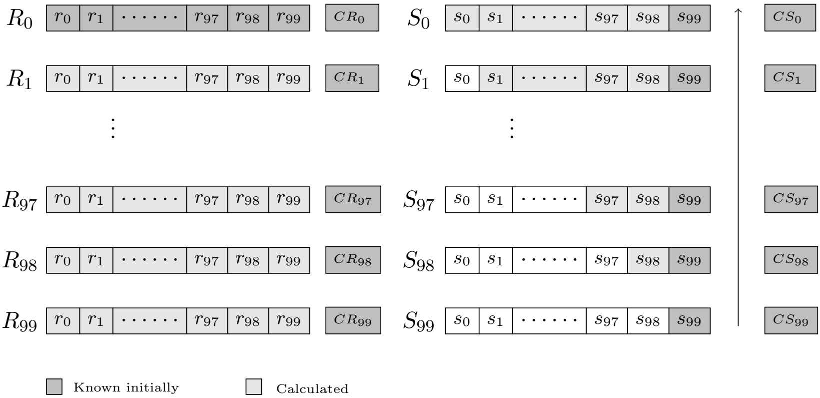
Notation

- $R_t, S_t \rightarrow$ States of the R, S registers at time t.
- $r_i^t,\ s_i^t \rightarrow i^{th}$ bit of $R,\ S$ at time t.
- $r_i^{t+1} = \rho_i(R_t, S_t)$ and $s_i^{t+1} = \beta_i(R_t, S_t)$.
- $R_{t,\Delta r_\phi}(t_0), S_{t,\Delta r_\phi}(t_0) \rightarrow$ States of the $R,\ S$ at time t, with fault in location ϕ of R at time t_0.
- $z_{i,\Delta r_\phi}(t_0) \rightarrow i$th key-stream bit, with fault in location ϕ of R at time t_0.
- $CR_t = r_{67}^t + s_{34}^t$ and $CS_t = r_{33}^t + s_{67}^t$.

Lemma 1 : Recovering R



Lemma 2 : Recovering S



Recovering the internal state

- The bits we require to deduce internal state

$$r_{99}^{t}, \; CR_t, \; s_{99}^{t}, \; CS_t, \quad \forall t \in [0, 99]$$

The functions θ_i

The key-stream bits $z_t, z_{t+1}, \ldots$ can be expressed as polynomial functions over R_t, S_t.

TABLE: The functions $z_i = \theta_i(R, S)$

i	$z_i = \theta_i(\cdot)$
0	$r_0 + s_0$
1	$r_0 \cdot r_{67} + r_0 \cdot s_{34} + r_{99} + s_{99}$
2	$r_0 \cdot r_{66} \cdot r_{67} + r_0 \cdot r_{66} \cdot s_{34} + r_0 \cdot r_{67} \cdot r_{99} + r_0 \cdot r_{67} \cdot s_{33} + r_0 \cdot r_{67} \cdot s_{34} \cdot s_{35} + r_0 \cdot r_{67} \cdot s_{34} + r_0 \cdot r_{67} + r_0 \cdot r_{99} \cdot s_{34} + r_0 \cdot s_{33} \cdot s_{34} + r_0 \cdot s_{34} \cdot s_{35} + r_{33} \cdot s_{99} + r_{66} \cdot r_{99} + r_{67} \cdot r_{99} \cdot s_{34} + r_{98} + r_{99} \cdot s_{33} + r_{99} \cdot s_{34} \cdot s_{35} + r_{99} \cdot s_{34} + r_{99} + s_{67} \cdot s_{99} + s_{98}$

Differentials properties of θ_i

$$
\begin{aligned}
&(1)\ \ \theta_1(\ldots, r_{67}, \ldots) + \theta_1(\ldots, 1 + r_{67}, \ldots) = r_0 \\
&(2)\ \ \theta_1(r_0, \ldots) + \theta_1(1 + r_0, \ldots) = s_{34} + r_{67} \\
&(3)\ \ \theta_2(\ldots, s_{99}) + \theta_2(\ldots, 1 + s_{99}) = s_{67} + r_{33}
\end{aligned}
$$

These differential properties have the following immediate implications.

$$z_{t+1} + z_{t+1,\Delta r_{67}}(t) = \theta_1(R_t, S_t) + \theta_1(R_{t,\Delta r_{67}}(t), S_{t,\Delta r_{67}}(t)) = r_0^t$$

$$z_{t+1} + z_{t+1,\Delta r_0}(t) = \theta_1(R_t, S_t) + \theta_1(R_{t,\Delta r_0}(t), S_{t,\Delta r_0}(t)) = s_{34}^t + r_{67}^t = CR_t$$

$$z_{t+2} + z_{t+2,\Delta s_{99}}(t) = \theta_2(R_t, S_t) + \theta_2(R_{t,\Delta s_{99}}(t), S_{t,\Delta s_{99}}(t)) = s_{67}^t + r_{33}^t = CS_t$$

Simplifying the attack

- From previous slide it is clear that if the attacker can reset the cipher each time and

  A. Fault locations $0, 67$ of R and 99 of S $\forall t \in [0, 99]$
  B. He is able to deduce $r_0^t,\ CR_t,\ CS_t$ $\forall t \in [0, 99]$

- He needs $r_{99}^t,\ s_{99}^t$ $\forall t \in [0, 99]$ to complete the attack.

- A is a very strong assumption, and will be only used to explain a few details of the attack.

Determining the rest of the state

- $s_0^t = z_t + r_0^t \; \forall t$.
- Note that $\beta_0(\cdot) = s_{99} \Rightarrow s_0^t = s_{99}^{t-1}$.
- Thus s_0^t for $t \in [1, 100]$ gives us the values for s_{99}^t for $t \in [0, 99]$
- $z_{t+1} = \theta_1(R_t, S_t) = CR_t \cdot r_0^t + r_{99}^t + s_{99}^t$

  $\Rightarrow r_{99}^t = z_{t+1} + CR_t \cdot r_0^t + s_{99}^t$.
- Now we have all bits required to complete the attack. Essentially implies that to complete the attack we need

$$r_0^t, \; CR_t, \; CS_t, \; \forall t \in [0, 99]$$

Random faults

- Adversary being able to fault specific locations of R, S is an impractical assumption.

Random faults

- Adversary being able to fault specific locations of R, S is an impractical assumption.
- In general, the attacker does not have control over the location of a random fault.

Random faults

- Adversary being able to fault specific locations of R, S is an impractical assumption.
- In general, the attacker does not have control over the location of a random fault.
- If a randomly applied fault toggles location ϕ of R, S, the attacker may try to guess ϕ by comparing the faulty and fault-free keystream sequences.

Signature vectors : [BMS 12]

- In [BMS 12], the differential keystream was compared with the first and second Signature vectors, to identify fault location for the Grain family.

$$\Psi^1_{r_\phi}[i] = \begin{cases} 1, & \text{if } z_{t+i} = z_{t+i,\Delta r_\phi}(t) \text{ for all choices of } R_t, S_t, \\ 0, & \text{otherwise.} \end{cases}$$

$$\Psi^2_{r_\phi}[i] = \begin{cases} 1, & \text{if } z_{t+i} \neq z_{t+i,\Delta r_\phi}(t) \text{ for all choices of } R_t, S_t, \\ 0, & \text{otherwise.} \end{cases}$$

- Let $\eta_{t,r_\phi}[i] = z_{t+i} + z_{t+i,\Delta r_\phi}(t)$
- The same idea fails for MICKEY, as multiple fault locations share the same signature vectors.

Signature vectors : Theorem 1

Theorem

The following statements hold

A. $\Psi^1_{r_\phi}[0] = 1, \forall \phi \in [1, 99]$ *and* $\Psi^2_{r_0}[0] = 1$.

B. $\Psi^1_{r_\phi}[0] = \Psi^1_{r_\phi}[1] = 1, \forall \phi \in [1, 99] \setminus \{67, 99\}$.

C. $\Psi^2_{r_{99}}[1] = 1$, *and* $\Psi^2_{r_{67}}[1] = 0$.

D. $\Psi^1_{s_\phi}[0] = 1, \forall \phi \in [1, 99]$ *and* $\Psi^2_{s_0}[0] = 1$.

E. $\Psi^1_{s_\phi}[0] = \Psi^1_{s_\phi}[1] = 1, \forall \phi \in [1, 99] \setminus \{34, 99\}$.

F. $\Psi^2_{s_{99}}[1] = 1$, *and* $\Psi^2_{s_{34}}[1] = 0$.

Proof

May be found in the Eprint version of the paper 2013/029.

Attack Scenario

- Adversary re-keys the device, injects a single fault at a random location of R at any PRGA round $t \in [0, 100]$.
- Repeat till 100 different faulty key-streams η_{t,r_ϕ} for 100 locations of R are obtained.
- By Coupon collector's Problem, this requires $\sim 100 \ln 100$ faults for each $t \in [0, 100]$.
- Total of $101 \cdot 100 \ln 100 = 2^{15.7}$ faults.
- Now for each t, attacker has 100 distinct differential keystreams. However he does not know which stream corresponds to which fault location.

Implication of A.

$$\mathbf{A}:\Psi^1_{r_\phi}[0] = 1, \forall \phi \in [1, 99] \text{ an } \Psi^2_{r_0}[0] = 1$$

- $\Psi^2_{r_0}[0] = 1 \Rightarrow \exists$ at least one stream s.t. $\eta_{t,r_\phi}[0] = 1$.
- $\Psi^1_{r_\phi}[0] = 1$ for all $\phi \neq 0 \Rightarrow \exists$ at most one stream s.t. $\eta_{t,r_\phi}[0] = 1$.
- So for any t the $\#$ of streams with $\eta_{t,r_\phi}[0] = 1$ is exactly 1.
- This stream must have been produced due to fault on r_0. Recall that

  $$z_{t+1} + z_{t+1,\Delta r_0}(t) = \theta_1(R_t, S_t) + \theta_1(R_{t,\Delta r_0}(t), S_{t,\Delta r_0}(t)) = s^t_{34} + r^t_{67} = CR_t$$
- Repeating the above logic for all t, we obtain all values of CR_t.

Implication of B, C

$$\textbf{B}: \Psi^1_{r_\phi}[0] = \Psi^1_{r_\phi}[1] = 1, \forall \phi \in [1, 99] \setminus \{67, 99\}$$
$$\textbf{C}: \Psi^2_{r_{99}}[1] = 1, \text{ and } \Psi^2_{r_{67}}[1] = 0$$

- **B** $\Rightarrow$ of the remaining 99 streams, atleast 97 satisfy

$$\text{(P1) } \eta_{t,r_\phi}[0] = \eta_{t,r_\phi}[1] = 0.$$

- **C** $\Rightarrow$ at least 1 and at most 2 satisfy

$$\text{(P2) } \eta_{t,r_\phi}[0] = 0, \eta_{t,r_\phi}[1] = 1.$$

- Recall that $\eta_{t,r_{67}}[1]$ is given by

$$z_{t+1} + z_{t+1,\Delta r_{67}}(t) = \theta_1(R_t, S_t) + \theta_1(R_{t,\Delta r_{67}}(t), S_{t,\Delta r_{67}}(t)) = r_0^t$$

- If # P1 $= 98$ and # P2 $= 1$ $\Rightarrow$ the P2 stream must have been produced due to fault on r_{99}. $\Rightarrow \eta_{t,r_{67}}[1] = 0 \Rightarrow r_0^t = 0$.
- If # P1 $= 97$ and # P2 $= 2$ $\Rightarrow$ the P2 streams must have been produced due to faults on r_{99}, r_{67}. $\Rightarrow \eta_{t,r_{67}}[1] = 1 \Rightarrow r_0^t = 1$.

Faults on S : Implication of D

- The same as **A** for faults on S.
- Exactly one stream has the property

$$\eta_{t,s_\phi}[0] = 1$$

- This must have been produced due to fault on s_0.
- No other information is gained.

Faults on S : Implication of E, F

- **E** $\Rightarrow$ of the remaining 99 streams, atleast 97 satisfy

$$\text{(P3) } \eta_{t,s_\phi}[0] = \eta_{t,s_\phi}[1] = 0.$$

- **F** $\Rightarrow$ at least 1 and at most 2 satisfy

$$\text{(P4) } \eta_{t,s_\phi}[0] = 0, \eta_{t,s_\phi}[1] = 1.$$

- Recall that $\eta_{t,s_{99}}[2]$ is given by

$$z_{t+2} + z_{t+2,\Delta s_{99}}(t) = \theta_2(R_t, S_t) + \theta_2(R_{t,\Delta s_{99}}(t), S_{t,\Delta s_{99}}(t)) = CS_t$$

- If # P3 = 98 and # P4 = 1 $\Rightarrow$ the P4 stream must have been produced due to fault on s_{99}. $\Rightarrow$ $\eta_{t,s_{99}}[2] = CS_t$.

Faults on S : Implication of E, F contd.

- If # P3 = 97 and # P4 = 2 $\Rightarrow$ the P4 streams must have been produced due to fault on s_{99}, s_{34}.

  (i) If the bit indexed 2 of these streams are equal $\Rightarrow CS_t = \eta_{t,s_{99}}[2] = \eta_{t,s_{34}}[2]$

  (ii) If the bit indexed 2 of these streams are unequal, no conclusions can be drawn.

- Under randomness assumptions, Pr[(ii) occurs] $= \frac{1}{4}$.

- Let $\gamma =$ number of undecided CS_t's in $[0, 100]$. Then

$$\gamma \sim \mathit{Binomial}(101, \frac{1}{4}) \Rightarrow E(\gamma) = 25.25$$

- Strategy : guess the undecided CS_t's $\Rightarrow$ Comp. burden 2^{γ}.

Complexity of Attack

- Fault requirement for R : $2^{15.7}$. Same for S.
- Total fault requirement : $2^{16.7}$
- Computational burden comes from guessing γ values of CS_t where

$$\gamma \sim \mathit{Binomial}(101, \frac{1}{4})$$

- Time complexity $\approx 2^{32.5}$.

CONCLUSION

- A differential fault attack on Mickey 2.0 using
  - using faults at chosen locations
  - using faults at random and unknown locations
- DFA against all 3 hardware candidates of eStream portfolio now reported.

Cipher	State size	Average # of Faults
Trivium	288	3.2
Grain v1	160	$\approx 2^{8.5}$
MICKEY 2.0	200	$\approx 2^{16.7}$

- MICKEY requires more faults because of complex structure.
- The attack can be extended to cases where a single fault injection affects multiple bits.

THANK YOU