Strengthening the $E_0$ Keystream Generator against Correlation Attacks and Algebraic Attacks

Frederik Armknecht
Matthias Krause
Dirk Stegemann

Theoretical Computer Science
University of Mannheim, Germany

3. GI-Kryptotag
September 15th, 2005
Overview

1. Introduction

2. Design Principles against Correlation Attacks and Algebraic Attacks

3. Application to $E_0$

4. Conclusion
**The E₀ Stream Cipher**

In each clock $t > 0$

- Produce keybit:
  
  $$z_t = \alpha(X_t) \oplus \beta(C_t)$$
  
  $$\alpha(X_t) = X_t^1 \oplus X_t^2 \oplus X_t^3 \oplus X_t^4$$
  
  $$\beta(C_t) = C_t^2$$

- Update memory bits:
  
  $$C_{t+1} = \delta(C_t, X_t)$$

Initialization in $t = 0$

- $n$-bit secret key $\mathcal{K}$
  
  $\rightarrow$ Bitstream Generator

- (public) initial value $C_0$
  
  $\rightarrow$ Memory
Correlation Attacks and Algebraic Attacks

... exploit equations in internal bits and corresponding output bits

\[ F(X_t, \ldots, X_{t+r-1}, Z_t, \ldots, Z_{t+r-1}) = 0 \]

in order to recover the secret key \( \mathcal{K} \).

correlation attacks:
- \( \text{deg}(F) = 1 \)
- equations \( F \) biased, i.e. true with probability \( \frac{1}{2} + \lambda \), \( \lambda \neq 0 \)

algebraic attacks:
- \( \text{deg}(F) = d > 1 \)
- equations \( F \) true with probability 1
A Correlation attack on $E_0$

Idea:
- output bits are computed as $z_t = \alpha(X_t) \oplus \beta(C_t)$
- look for biased linear combinations of the $\beta(C_t)$

More precisely: Find $\gamma = (\gamma_0, \ldots, \gamma_{r-1}) \in \{0, 1\}^r$ such that

$$\lambda(\gamma) = \left( Pr \left[ \bigoplus_{i=0}^{r-1} \gamma_i \cdot \beta(C_{t+i}) = 0 \right] - Pr \left[ \bigoplus_{i=0}^{r-1} \gamma_i \cdot \beta(C_{t+i}) = 1 \right] \right) \neq 0$$

**Theorem (Lu, Vaudenay 2004)**

For the $E_0$ generator, it holds that $\lambda_{\text{max}}(\gamma) = \frac{25}{256}$ for $r \leq 25$. 
An Algebraic attack on $E_0$

Scenario:
- $\varphi$ many $Z$-functions $F_Z$ of degree $d$ for each clock $t$ fulfilling
  $$F_Z(X_t, \ldots, X_{t+r-1}) = 0$$
  for each $Z = (z_t, \ldots, z_{t+r-1}) \in \{0, 1\}^r$
- number of equations $\approx$ number of monomials $\approx \binom{n}{d}$

Theorem (Armknecht, Krause 2003)

*For the $E_0$ generator, $\exists$ $Z$-functions with $d = 4$ and $r = 4$.***
Complexities of the two Attacks on $E_0$

<table>
<thead>
<tr>
<th></th>
<th>Correlation Attack</th>
<th>Algebraic Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>$m$</strong></td>
<td>$m = \max\left{ \frac{1}{\lambda^{10}}, \frac{236.59}{\lambda^{8}} \right}$</td>
<td>$O\left(\binom{n}{d}/\varphi\right)$</td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td>$24m$</td>
<td>$O\left(\binom{n}{d}^3\right)$</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>$36m + 3 \cdot 2^{18} \cdot \min{m, 2^{18}}$</td>
<td>$O\left(\binom{n}{d}^2\right)$</td>
</tr>
<tr>
<td><strong>Space</strong></td>
<td>$m$</td>
<td>$O\left(\binom{n}{d}^2\right)$</td>
</tr>
</tbody>
</table>

$\Rightarrow$ In order to improve security

- $|\lambda| \rightarrow \min$
- $d \rightarrow \max$
Countermeasures against Correlation Attacks

Theorem

If for all $1 \leq t \leq r$

- $z_t = \alpha_t(X_t) \oplus \beta_t(C_t)$, $\beta_t \not\equiv 0$ for at least one $t$
- all $X_t$ independent
- $\beta_t \not\equiv 0 \Rightarrow \beta_t$ balanced, i.e. $|\beta_t^{-1}(0)| = |\beta_t^{-1}(1)|$
- $\delta$ balanced, i.e. $\Pr[C \rightarrow C']$ is equal for all $C, C'$

then $\lambda (\beta_1(C_1) \oplus \ldots \oplus \beta_r(C_r)) = 0$.

In the case of $E_0$:

- $\checkmark$ $z_t = \underbrace{X_1^t \oplus X_2^t \oplus X_3^t \oplus X_4^t}_{\alpha(X_t)} \oplus \underbrace{C_2^t}_{\beta(C_t)}$
- $\checkmark$ $X_t$ independent for $r \leq 25$
- $\checkmark$ $\beta$ balanced
- $\oplus$ $\delta$ not balanced
Countermeasures against Algebraic Attacks

Definition
For a subset $A \subseteq \{0, 1\}^n$,
- we denote by $Ann(A)$ the set of all Boolean functions $f : \{0, 1\}^n \rightarrow \{0, 1\}$ such that $f(x) = 0$ for all $x \in A$
- we define $\text{mindeg}(A) = \min\{\deg(f) : f \in Ann(A)\}$

Theorem
If for all $1 \leq t \leq r$
- $z_t = \alpha(X_t) \oplus \beta(C_t)$
- all $X_t$ independent
- $\text{mindeg}(\alpha^{-1}(0)) = \text{mindeg}(\alpha^{-1}(1)) = d$
then $\deg(F_Z) \geq d$. 
Countermeasures against Algebraic Attacks

In the case of $E_0$: $\text{mindeg}(\alpha^{-1}(1)) = \text{mindeg}(\alpha^{-1}(0)) = 1$

Idea: Find a function $\alpha$ with $\text{mindeg}(\alpha^{-1}(0))$ and $\text{mindeg}(\alpha^{-1}(1))$ as large as possible.

How large is the largest possible?
Lemma

For each Boolean function $\alpha : \{0, 1\}^k \rightarrow \{0, 1\}$,

$$\mindeg(\alpha^{-1}(0)), \mindeg(\alpha^{-1}(1)) \leq \left\lceil \frac{k}{2} \right\rceil$$

This bound is matched by the majority function:

Corollary

For the Function

$$maj : \{0, 1\}^k \rightarrow \{0, 1\}$$

$$x \mapsto \begin{cases} 0 & \text{weight}(x) \leq \lfloor k/2 \rfloor \\ 1 & \text{otherwise} \end{cases}$$

(Similarly for $k$ even)

it holds that $\mindeg(\text{maj}^{-1}(0)) = \mindeg(\text{maj}^{-1}(1)) = \left\lceil \frac{k}{2} \right\rceil$
Improving $E_0$

Increase resistance

... against correlation attacks by decreasing $\lambda$

- Replace $\delta$ by a balanced function $\rightarrow \lambda = 0$ for $r \leq 25$

... against algebraic attacks by increasing $\min\{\deg(F_Z)\}$

- Replace $\alpha(X_t)$ by $\text{maj}(X_t) \rightarrow \deg(F_Z) \geq 2$ for $r \leq 25$
## Improved Variants of $E_0$

<table>
<thead>
<tr>
<th>$E_0$</th>
<th>$\alpha(X_t)$</th>
<th>$\beta(C_t)$</th>
<th>$\delta(X_t, C_t)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\oplus X_t^i$</td>
<td>$C_t^2$</td>
<td>original</td>
<td></td>
</tr>
<tr>
<td>$E_0^1$</td>
<td>$maj(X_t)$</td>
<td>$C_t^2$</td>
<td>$X_t + C_t$</td>
</tr>
<tr>
<td>$E_0^2$</td>
<td>$maj(X_t)$</td>
<td>$maj(C_t)$</td>
<td>$X_t + C_t$</td>
</tr>
<tr>
<td>$E_0^3$</td>
<td>$\oplus X_t^i$</td>
<td>$C_t^2 \oplus C_t^3 \oplus C_t^4$</td>
<td>original</td>
</tr>
<tr>
<td>$E_0^4$</td>
<td>$\oplus X_t^i$</td>
<td>$C_t^1 \oplus C_t^3 \oplus C_t^4$</td>
<td>original</td>
</tr>
</tbody>
</table>

The favourite candidates:

- $E_0^2$: highest resistance
- $E_0^4$: significant improvement with only small changes
Conclusion

- Theoretical design principles against certain types of
  - correlation attacks
  - algebraic attacks

- Application to the \( E_0 \) generator yields
  - significantly improved resistance against these attacks
  - with only small changes of the design
Thank you!

{frederik.armknecht, matthias.krause, dirk.stegemann}
@th.informatik.uni-mannheim.de