Nonlinear Equivalence of Stream Ciphers

Sondre Rønjom and **Carlos Cid**

Norwegian National Security Authority (NSM)
Royal Holloway, University of London

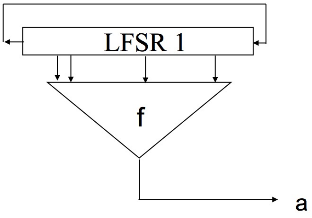
FSE 2010
08 Feb 2010

Filter Generator

Information Security Group

A filter generator over $\mathbb{F}_2$ is a stream cipher in perhaps its simplest form, with a well-defined mathematical description:

- it consists of a sequence generator (e.g. LFSR) and a Boolean function f, which work together to produce as output a binary string (keystream) based on the state of the register.



Filter Generator Security

The security of filter generators is highly reliant on both the properties of the sequence-generator, as well as the properties of the Boolean function.

Filter Generator Security

Information Security Group

The security of filter generators is highly reliant on both the properties of the sequence-generator, as well as the properties of the Boolean function.

- For instance, based on the algebraic normal form of a Boolean function, related properties such as algebraic immunity, algebraic degree, nonlinearity and correlation immunity, can be computed to derive some of the cipher's security.

Filter Generator Security

Information Security Group

The security of filter generators is highly reliant on both the properties of the sequence-generator, as well as the properties of the Boolean function.

- For instance, based on the algebraic normal form of a Boolean function, related properties such as algebraic immunity, algebraic degree, nonlinearity and correlation immunity, can be computed to derive some of the cipher's security.
- Likewise, we know that the Hamming weight of a characteristic polynomial should not be low in order to resist correlation attacks.

Filter Generator Security

The security of filter generators is highly reliant on both the properties of the sequence-generator, as well as the properties of the Boolean function.

- For instance, based on the algebraic normal form of a Boolean function, related properties such as algebraic immunity, algebraic degree, nonlinearity and correlation immunity, can be computed to derive some of the cipher's security.
- Likewise, we know that the Hamming weight of a characteristic polynomial should not be low in order to resist correlation attacks.
- And to resist inversion attacks, the positions of the cipher's LFSR which a Boolean function taps from, should satisfy additional requirements.

Filter Generator Security

The security of filter generators is highly reliant on both the properties of the sequence-generator, as well as the properties of the Boolean function.

- For instance, based on the algebraic normal form of a Boolean function, related properties such as algebraic immunity, algebraic degree, nonlinearity and correlation immunity, can be computed to derive some of the cipher's security.
- Likewise, we know that the Hamming weight of a characteristic polynomial should not be low in order to resist correlation attacks.
- And to resist inversion attacks, the positions of the cipher's LFSR which a Boolean function taps from, should satisfy additional requirements.

However, the two components are usually analysed **separately**.

Filter Generator Security

Information Security Group

Perhaps this form of analysis has its limitations:

- For example, in algebraic attacks, one collects polynomials arising from the cipher output.

Filter Generator Security

Information Security Group

Perhaps this form of analysis has its limitations:

- For example, in algebraic attacks, one collects polynomials arising from the cipher output.
- Analysis (solving) estimates then consider this set as a random set of polynomials.

Filter Generator Security

Perhaps this form of analysis has its limitations:

- For example, in algebraic attacks, one collects polynomials arising from the cipher output.
- Analysis (solving) estimates then consider this set as a random set of polynomials.
- However, it has been shown that this set is very structured: for every monomial, the sequence of coefficients has a minimal polynomial which can be derived from the **LFSR** and the **Boolean function** [RH07].

Stream Cipher Equivalence

We consider (nonlinear) equivalence of LFSR-based stream ciphers using basic properties of Galois fields.

- We thus construct **isomorphism classes** of stream ciphers.
  - The topic has been studied before in the context of block ciphers (e.g. [BB02], [MR02]).

Stream Cipher Equivalence

We consider (nonlinear) equivalence of LFSR-based stream ciphers using basic properties of Galois fields.

- We thus construct **isomorphism classes** of stream ciphers.
  - The topic has been studied before in the context of block ciphers (e.g. [BB02], [MR02]).
- In our case, we show however that several important cryptographic properties, such as nonlinearity and algebraic immunity, are **not invariant** with respect to such equivalence classes.

Stream Cipher Equivalence

Information Security Group

Our Conclusions:

- analysis of both the generator and the corresponding Boolean function should be combined when assessing the security of a filter generator.
- furthermore, any cryptographic property should be defined with respect to the weakest equivalent cipher.
- however this seems very hard for filter generators used in practice, since the class of equivalent ciphers is very large in these cases.

Linear Feedback Shift Register

Information Security Group

Let **s** be the output of LFSR $\mathcal{L}$ over $\mathbb{F}_2$, with (primitive) characteristic polynomial $c(x)$ of degree n.
Let $\alpha \in \mathbb{F}_{2^n}$ be a root of $c(x)$.

Linear Feedback Shift Register

Let **s** be the output of LFSR $\mathcal{L}$ over $\mathbb{F}_2$, with (primitive) characteristic polynomial $c(x)$ of degree n.
Let $\alpha \in \mathbb{F}_{2^n}$ be a root of $c(x)$.

Then **s** may be written over $\mathbb{F}_{2^n}$ in terms of the roots of $c(x)$ as

$$s_t = \mathrm{Tr}(X\alpha^t) = \sum_{i=0}^{n-1} (X\alpha^t)^{2^i}, \quad t = 0, 1, 2, \ldots,$$

where the $2^n - 1$ nonzero choices of $X \in \mathbb{F}_{2^n}^*$ result in $2^n - 1$ distinct shifts of the same m-sequence **s**.

Linear Feedback Shift Register

Let **s** be the output of LFSR $\mathcal{L}$ over $\mathbb{F}_2$, with (primitive) characteristic polynomial $c(x)$ of degree n.
Let $\alpha \in \mathbb{F}_{2^n}$ be a root of $c(x)$.

Then **s** may be written over $\mathbb{F}_{2^n}$ in terms of the roots of $c(x)$ as

$$s_t = \mathrm{Tr}(X\alpha^t) = \sum_{i=0}^{n-1} (X\alpha^t)^{2^i}, \quad t = 0, 1, 2, \ldots,$$

where the $2^n - 1$ nonzero choices of $X \in \mathbb{F}_{2^n}^*$ result in $2^n - 1$ distinct shifts of the same m-sequence **s**.

Remark: α is a generator of $\mathbb{F}_{2^n}^*$. If β is another generator, we will use the mapping $\alpha \mapsto \beta$ to define another sequence generator.

Example

Let $n = 5, q = 2^n = 32$ and let $\mathbb{F}_2(\alpha) \simeq \mathbb{F}_{32}$, where

$$m_\alpha(x) = x^5 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$$

is a primitive polynomial.
An m-sequence $\mathbf{s}$ can be generated as

$$s_t = \mathrm{Tr}(X\alpha^t), t = 0, 1, 2, \ldots,$$

where $X \in \mathbb{F}_{32}^*$.

Example

Information Security Group

Let $n = 5, q = 2^n = 32$ and let $\mathbb{F}_2(\alpha) \simeq \mathbb{F}_{32}$, where

$$m_\alpha(x) = x^5 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$$

is a primitive polynomial.
An m-sequence **s** can be generated as

$$s_t = \mathrm{Tr}(X\alpha^t), t = 0, 1, 2, \ldots,$$

where $X \in \mathbb{F}_{32}^*$. Now let $\beta = \alpha^{21}$ and $X^{21} = Y \in \mathbb{F}_2(\beta)$. It follows that

$$\mathrm{Tr}(X\alpha^t) = \mathrm{Tr}((Y\beta^t)^3), t = 0, 1, 2, \ldots,$$

since $3 \cdot 21 \equiv 1 \pmod{31}$.

Example (cont.)

We can use the LFSR with characteristic polynomial $m_\beta(x)$ to generate the sequence $\mathbf{s}$.

- However we need to combine its state in a non-linear way.

Example (cont.)

We can use the LFSR with characteristic polynomial $m_\beta(x)$ to generate the sequence $\mathbf{s}$.

- However we need to combine its state in a non-linear way.

The corresponding sequence generator over $\mathbb{F}_2(\beta)$ is given by

$$s_t = f(b_t, b_{t+1}, \dots, b_{t+4}), t = 0, 1, 2, \dots,$$

where

$$(b_t, b_{t+1}, \dots, b_{t+4}) = (\mathrm{Tr}(Y\beta^t), \mathrm{Tr}(Y\beta^{t+1}), \dots, \mathrm{Tr}(Y\beta^{t+4})),$$

and

$$f(x_0, x_1, x_2, x_3, x_4) = x_0x_2 + x_2x_3 + x_1x_4 + x_2x_4 + x_1 + x_3.$$

Example (cont.)

We can use the LFSR with characteristic polynomial $m_\beta(x)$ to generate the sequence $\mathbf{s}$.

- However we need to combine its state in a non-linear way.

The corresponding sequence generator over $\mathbb{F}_2(\beta)$ is given by

$$s_t = f(b_t, b_{t+1}, \ldots, b_{t+4}), t = 0, 1, 2, \ldots,$$

where

$$(b_t, b_{t+1}, \ldots, b_{t+4}) = (\mathrm{Tr}(Y\beta^t), \mathrm{Tr}(Y\beta^{t+1}), \ldots, \mathrm{Tr}(Y\beta^{t+4})),$$

and

$$f(x_0, x_1, x_2, x_3, x_4) = x_0x_2 + x_2x_3 + x_1x_4 + x_2x_4 + x_1 + x_3.$$

The two filter generators (one of them is linear) will generate identical sequences for all possible initial states X and $Y = X^{21}$, and they are thus equivalent sequence generators.

Equivalence of Filter Generators

Information Security Group

The basic idea: let α, β be generators of $\mathbb{F}^*_{2^n}$:

Equivalence of Filter Generators

The basic idea: let α, β be generators of $\mathbb{F}_{2^n}^*$:

$$\alpha \quad \alpha^2 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5 \quad \alpha^6 \quad \dots \quad \alpha^{2^n-2} \quad \alpha^{2^n-1}$$

Equivalence of Filter Generators

The basic idea: let α, β be generators of $\mathbb{F}^*_{2^n}$:

$$
\begin{array}{cccccccccc}
\alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \ldots & \alpha^{2^n-2} & \alpha^{2^n-1} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \vdots & \downarrow & \downarrow \\
f(\alpha) & f(\alpha^2) & f(\alpha^3) & f(\alpha^4) & f(\alpha^5) & f(\alpha^6) & \ldots & f(\alpha^{2^n-2}) & f(\alpha^{2^n-1}) \\
\Downarrow & \Downarrow & \Downarrow & \Downarrow & \Downarrow & \Downarrow & \vdots & \Downarrow & \Downarrow \\
0 & 0 & 1 & 0 & 1 & 1 & \cdots & 0 & 1
\end{array}
$$

Equivalence of Filter Generators

Information Security Group

The basic idea: let α, β be generators of $\mathbb{F}_{2^n}^*$:

$$
\begin{array}{cccccccccc}
\alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \dots & \alpha^{2^n-2} & \alpha^{2^n-1} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \vdots & \downarrow & \downarrow \\
f(\alpha) & f(\alpha^2) & f(\alpha^3) & f(\alpha^4) & f(\alpha^5) & f(\alpha^6) & \dots & f(\alpha^{2^n-2}) & f(\alpha^{2^n-1}) \\
\Downarrow & \Downarrow & \Downarrow & \Downarrow & \Downarrow & \Downarrow & \vdots & \Downarrow & \Downarrow \\
0 & 0 & 1 & 0 & 1 & 1 & \cdots & 0 & 1
\end{array}
$$

$$
\begin{array}{cccccccccc}
\beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \dots & \beta^{2^n-2} & \beta^{2^n-1}
\end{array}
$$

Equivalence of Filter Generators

The basic idea: let α, β be generators of $\mathbb{F}^*_{2^n}$:

$$
\begin{array}{cccccccccc}
\alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \dots & \alpha^{2^n-2} & \alpha^{2^n-1} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \vdots & \downarrow & \downarrow \\
f(\alpha) & f(\alpha^2) & f(\alpha^3) & f(\alpha^4) & f(\alpha^5) & f(\alpha^6) & \dots & f(\alpha^{2^n-2}) & f(\alpha^{2^n-1}) \\
\Downarrow & \Downarrow & \Downarrow & \Downarrow & \Downarrow & \Downarrow & \vdots & \Downarrow & \Downarrow \\
0 & 0 & 1 & 0 & 1 & 1 & \cdots & 0 & 1 \\
\Uparrow & \Uparrow & \Uparrow & \Uparrow & \Uparrow & \Uparrow & \vdots & \Uparrow & \Downarrow \\
g(\beta) & g(\beta^2) & g(\beta^3) & g(\beta^4) & g(\beta^5) & g(\beta^6) & \dots & g(\beta^{2^n-2}) & g(\beta^{2^n-1}) \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \vdots & \uparrow & \uparrow \\
\beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \dots & \beta^{2^n-2} & \beta^{2^n-1}
\end{array}
$$

Equivalence of Filter Generators

Information Security Group

The basic idea: let α, β be generators of $\mathbb{F}_{2^n}^*$:

$$
\begin{array}{cccccccccc}
\alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \dots & \alpha^{2^n-2} & \alpha^{2^n-1} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \vdots & \downarrow & \downarrow \\
f(\alpha) & f(\alpha^2) & f(\alpha^3) & f(\alpha^4) & f(\alpha^5) & f(\alpha^6) & \dots & f(\alpha^{2^n-2}) & f(\alpha^{2^n-1}) \\
\Downarrow & \Downarrow & \Downarrow & \Downarrow & \Downarrow & \Downarrow & \vdots & \Downarrow & \Downarrow \\
0 & 0 & 1 & 0 & 1 & 1 & \cdots & 0 & 1 \\
\Uparrow & \Uparrow & \Uparrow & \Uparrow & \Uparrow & \Uparrow & \vdots & \Uparrow & \Downarrow \\
g(\beta) & g(\beta^2) & g(\beta^3) & g(\beta^4) & g(\beta^5) & g(\beta^6) & \dots & g(\beta^{2^n-2}) & g(\beta^{2^n-1}) \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \vdots & \uparrow & \uparrow \\
\beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \dots & \beta^{2^n-2} & \beta^{2^n-1}
\end{array}
$$

Note that the truth table is not complete: we do not have the image of $0 \in \mathbb{F}_{2^n}$. Thus there are equivalent functions $\overline{f}, \overline{g}$ which could also be used.

Equivalence - definitions

Information Security Group

Definition

For a sequence $\mathbf{s} \in \mathbb{F}_2^{q-1}$ and $\beta \in \mathbb{F}_q^*$, let

$$V_\beta(\mathbf{s}) = \{f \in \mathbb{B}_n \mid \mathbf{s} \in \mathcal{L}_\beta(f)\}.$$

We can consider $V_\beta(\mathbf{s})$ as the set of all filter generators with characteristic polynomial $g_\beta(x)$ that generate $\mathbf{s}$ as its first $q-1$ terms.

Equivalence - definitions

Definition

For a sequence $\mathbf{s} \in \mathbb{F}_2^{q-1}$ and $\beta \in \mathbb{F}_q^*$, let

$$V_\beta(\mathbf{s}) = \{f \in \mathbb{B}_n \mid \mathbf{s} \in \mathcal{L}_\beta(f)\}.$$

We can consider $V_\beta(\mathbf{s})$ as the set of all filter generators with characteristic polynomial $g_\beta(x)$ that generate $\mathbf{s}$ as its first $q-1$ terms.

Definition

Let $\mathbf{s} \in \mathbb{F}_2^{q-1}$ be a sequence with period e dividing $q-1$, where e is not a divisor of $2^k - 1$, with $0 < k < n$. Then let

$$\mathbb{G}_n(\mathbf{s}) = \{V_\beta(\mathbf{s}) \,|\, \beta \in \mathbb{F}_q, \;\; e \,|\, ord(\beta)\}.$$

In other words, the set $\mathbb{G}_n(\mathbf{s})$ may be viewed as a class of filter generators of length n that generate $\mathbf{s}$ as a keystream.

Number of Equivalent Filter Generators

Information Security Group

Lemma

Let $\mathbf{s} \in \mathbb{F}_2^{q-1}$ *denote a periodic sequence with* $e = per(\mathbf{s})$ *and* $\beta \in \mathbb{F}_q^*$ *where* $per(\mathbf{s}) \mid ord(\beta)$. *Then*

$$|V_\beta(\mathbf{s})| \leq \frac{e(q-1)}{ord(\beta)} \cdot 2^{q-ord(\beta)}.$$

Number of Equivalent Filter Generators

Information Security Group

Lemma

Let $\mathbf{s} \in \mathbb{F}_2^{q-1}$ *denote a periodic sequence with* $e = per(\mathbf{s})$ *and* $\beta \in \mathbb{F}_q^*$ *where* $per(\mathbf{s}) \,|\, ord(\beta)$*. Then*

$$|V_\beta(\mathbf{s})| \leq \frac{e(q-1)}{ord(\beta)} \cdot 2^{q-ord(\beta)}.$$

In the case of more interest ($ord(\beta) = q - 1$): we have equality and there are 2 elements in $V_\beta(\mathbf{s})$ (except for affine equivalence).

Number of Equivalent Filter Generators

Information Security Group

Lemma

Let $\mathbf{s} \in \mathbb{F}_2^{q-1}$ *denote a periodic sequence with* $e = per(\mathbf{s})$ *and* $\beta \in \mathbb{F}_q^*$ *where* $per(\mathbf{s}) \mid ord(\beta)$. *Then*

$$|V_\beta(\mathbf{s})| \leq \frac{e(q-1)}{ord(\beta)} \cdot 2^{q-ord(\beta)}.$$

In the case of more interest ($ord(\beta) = q - 1$): we have equality and there are 2 elements in $V_\beta(\mathbf{s})$ (except for affine equivalence).

Theorem

If $\mathbf{s} \in \mathbb{F}_2^{q-1}$ *has period* $q - 1$, *then*

$$|\mathbb{G}_n(\mathbf{s})| = \phi(q-1)/n,$$

where $\phi(q-1)$ *is the number of generators of* $\mathbb{F}_q^*$.

Another Example I

Information Security Group

Consider the binary sequence

$$\mathbf{s} = (1011111101000100110001010110001),$$

of length 31.

Another Example I

Consider the binary sequence

$$\mathbf{s} = (1011111101000100110001010110001),$$

of length 31.
There are $\phi(31)/5 = 6$ primitive polynomials over $\mathbb{F}_2$ of degree 5.

Another Example I

Consider the binary sequence

$$\mathbf{s} = (1011111101000100110001010110001),$$

of length 31.

There are $\phi(31)/5 = 6$ primitive polynomials over $\mathbb{F}_2$ of degree 5.

For each (distinct) generator β of the multiplicative group of $\mathbb{F}(\alpha)$, we compute a function f_β such that $\mathbf{s} \in \mathcal{L}_\beta(f_\beta)$, where we let $g_\alpha = x^5 + x^2 + 1$.

Another Example I

Information Security Group

Consider the binary sequence

$$\mathbf{s} = (1011111101000100110001010110001),$$

of length 31.
There are $\phi(31)/5 = 6$ primitive polynomials over $\mathbb{F}_2$ of degree 5.
For each (distinct) generator β of the multiplicative group of $\mathbb{F}(\alpha)$, we compute a function f_β such that $\mathbf{s} \in \mathcal{L}_\beta(f_\beta)$, where we let $g_\alpha = x^5 + x^2 + 1$.
The distinct nonzero coset-leaders modulo 31 are $K = \{1, 3, 5, 7, 11, 15\}$, and thus we may compute six functions $f_{\alpha_k}, k \in K$, where we let $\alpha_k = \alpha^k$ and pick one function f_{α_k} from each class $V_{\alpha_k} \in \mathbb{G}_5(\mathbf{s})$.

Another Example II

Information Security Group

We have 6 functions $f_{\alpha_k} \in V_{\alpha_k}(\mathbf{s}) \in \mathbb{G}_5(\mathbf{s}), k \in K$:

$$
\begin{aligned}
f_{\alpha_1} &= x_0x_1x_2x_3 + x_0x_1x_2x_4 + x_0x_1x_3x_4 + x_1x_2x_3x_4 + x_0x_1x_2 + x_0x_1x_3 + \\
&\quad x_0x_2x_3 + x_1x_2x_3 + x_0x_1x_4 + x_2x_3x_4 + x_0x_2 + x_0 + x_1 \\
f_{\alpha_3} &= x_0x_1x_2x_3 + x_0x_1x_3x_4 + x_1x_2x_3x_4 + x_0x_1x_2 + x_0x_1x_4 + x_0x_3x_4 + \\
&\quad x_1x_3x_4 + x_2x_3x_4 + x_0x_1 + x_1x_3 + x_2x_4 + x_2 + x_3 \\
f_{\alpha_5} &= x_0x_1x_2x_4 + x_0x_2x_3x_4 + x_1x_2x_3x_4 + x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + \\
&\quad x_1x_2x_3 + x_0x_1x_4 + x_0x_3x_4 + x_0x_2 + x_0x_4 + x_1x_4 + x_2x_4 + x_0 + \\
&\quad x_1 + x_2 + x_3 + x_4 \\
f_{\alpha_7} &= x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 + x_1x_2 + x_0x_3 + \\
&\quad x_0x_4 + x_1x_4 + x_3x_4 + x_0 + x_3 \\
f_{\alpha_{11}} &= x_0x_1x_2 + x_0x_2x_3 + x_1x_2x_3 + x_0x_1x_4 + x_1x_2x_4 + x_0x_1 + x_0x_2 + \\
&\quad x_1x_3 + x_0x_4 + x_2 \\
f_{\alpha_{15}} &= x_0x_1 + x_1x_2 + x_1x_3 + x_0x_4 + x_1x_4 + x_2x_4 + x_3x_4 + x_0 + x_1 + x_3
\end{aligned}
$$

Another Example III

Information Security Group

The columns of the table below are ordered by the 6 functions $f_{\alpha_k} \in V_{\alpha_k}(\mathbf{s}) \in \mathbb{G}_5(\mathbf{s}), k \in K$:

	f_{α_1}	f_{α_3}	f_{α_5}	f_{α_7}	$f_{\alpha_{11}}$	$f_{\alpha_{15}}$
n	5	5	5	5	5	5
d	4	4	4	3	3	2
w_H	16	16	16	16	16	16
NL	10	10	10	8	12	8
AI	2	3	2	2	3	2
CI	0	0	0	1	0	1

Note that, apart from the weight of the truth-tables and the number of variables, none of the other properties remain the same with respect to the transformations.

Cryptanalytic Implications

If we restrict ourselves to keystream-sequences of period $q - 1 = 2^n - 1$, which is the common case for sequences generated by filter generators, then there are $2 \cdot |\mathbb{G}_n(\mathbf{s})|$ isomorphic filter generators generating the same keystream sequence(s), excluding affine equivalence.

Cryptanalytic Implications

If we restrict ourselves to keystream-sequences of period $q - 1 = 2^n - 1$, which is the common case for sequences generated by filter generators, then there are $2 \cdot |\mathbb{G}_n(\mathbf{s})|$ isomorphic filter generators generating the same keystream sequence(s), excluding affine equivalence.

Thus, in order to assess the cryptographic properties of a filter generator, one should in theory check whether there exist in this class weak isomorphic ciphers with respect to some cryptographic property.

Cryptanalytic Implications

In particular, any cryptographic property **should** be defined with respect to the weakest cipher in the equivalence class.

Definition

Let $\mathcal{P}$ be a cryptographic measurement of a filter generator $\mathcal{S}$, which generates a sequence $\mathbf{s}$. Then the filter generator $\mathcal{S}$ is said to be $\mathcal{P}$-resistant only if there is no isomorphic filter generator $\mathcal{S}'$ with measurement $\mathcal{P}' < \mathcal{P}$.

We discuss in the paper a few concepts (e.g. Algebraic Immunity), but do not extend the analysis.

Cryptanalytic Implications

The bad news: at this stage, this is likely to have limited application in practice.

- for sizes used in practice, the number of elements in the equivalence classes is huge.
- filtering functions are likely to be hard to describe (very dense with many variables).

Cryptanalytic Implications

Information Security Group

The bad news: at this stage, this is likely to have limited application in practice.

- for sizes used in practice, the number of elements in the equivalence classes is huge.
- filtering functions are likely to be hard to describe (very dense with many variables).

Areas for further research include:

- studying classes of Boolean functions which are equivalent with respect to both nonlinear and linear equivalence.
- generalising the idea, and defining equivalence with respect to the set of all possible combiner-generators generating a periodic sequence.

Conclusions

Given a LFSR-based stream cipher $\mathcal{S}$ generating a sequence $\mathbf{s}$, we showed how to define an equivalence class $\mathbb{G}_n(\mathbf{s})$, consisting of all filter generators of length n that produce $\mathbf{s}$ as output (and in most cases of interest, of all filter generators equivalent to $\mathcal{S}$).

Conclusions

Given a LFSR-based stream cipher $\mathcal{S}$ generating a sequence $\mathbf{s}$, we showed how to define an equivalence class $\mathbb{G}_n(\mathbf{s})$, consisting of all filter generators of length n that produce $\mathbf{s}$ as output (and in most cases of interest, of all filter generators equivalent to $\mathcal{S}$).

- Somewhat surprisingly, several properties of cryptographic relevance are not invariant among the elements of $\mathbb{G}_n(\mathbf{s})$.

Conclusions

Information Security Group

Given a LFSR-based stream cipher $\mathcal{S}$ generating a sequence $\mathbf{s}$, we showed how to define an equivalence class $\mathbb{G}_n(\mathbf{s})$, consisting of all filter generators of length n that produce $\mathbf{s}$ as output (and in most cases of interest, of all filter generators equivalent to $\mathcal{S}$).

- Somewhat surprisingly, several properties of cryptographic relevance are not invariant among the elements of $\mathbb{G}_n(\mathbf{s})$.
- Thus, we feel that a security analysis is **incomplete** without considering the elements in $\mathbb{G}_n(\mathbf{s})$.
  - For example, one should not reach conclusions of the security properties of a filter generator by, for instance, analysing the algebraic degree or algebraic immunity of the corresponding Boolean function,
  - or the properties such as the weight of the polynomial defining the LFSR, or by the position of the registers that are tapped as input to the Boolean function.

Conclusions

In particular, our analysis makes it clear that one should not generally analyse the components of a stream cipher separately, as it is usual in practice.

Conclusions

In particular, our analysis makes it clear that one should not generally analyse the components of a stream cipher separately, as it is usual in practice.

As a result, the natural object of analysis seems to be the equivalence class $\mathbb{G}_n(\mathbf{s})$. The bad news is that this is likely to be hard in practice.

More research is required...

Conclusions

In particular, our analysis makes it clear that one should not generally analyse the components of a stream cipher separately, as it is usual in practice.

As a result, the natural object of analysis seems to be the equivalence class $\mathbb{G}_n(\mathbf{s})$. The bad news is that this is likely to be hard in practice.

More research is required...

Thank you!