Constructions of feebly secure cryptographic primitives

Olga Melanich

Steklov Institute of Mathematics at St. Petersburg

3.10.2009

Basic definitions

Notation

$B_{n,m} = \{f : B^n \to B^m\}$, where $B = \{0, 1\}$.

Basic definitions

Notation

$B_{n,m} = \{f : B^n \to B^m\}$, where $B = \{0, 1\}$.

Definition

Circuit complexity of a function f is the smallest number of gates in a circuit computing f (such circuit is called **an optimal circuit** for f)

$$C(f) = \min_{c : \forall x \, c(x) = f(x)} C(c).$$

Basic definitions

Notation

$B_{n,m} = \{f : B^n \to B^m\}$, where $B = \{0, 1\}$.

Definition

Circuit complexity of a function f is the smallest number of gates in a circuit computing f (such circuit is called **an optimal circuit** for f)

$$C(f) = \min_{c : \forall x\, c(x) = f(x)} C(c).$$

Definition

$f_n \in B_{n,m}$, injective. **The measure of feeble one-wayness** $M_F(f_n) = \frac{C(f_n^{-1})}{C(f_n)}$.

Basic definitions

Notation

$B_{n,m} = \{f : B^n \to B^m\}$, where $B = \{0, 1\}$.

Definition

Circuit complexity of a function f is the smallest number of gates in a circuit computing f (such circuit is called **an optimal circuit** for f)

$$C(f) = \min_{c:\forall x\, c(x)=f(x)} C(c).$$

Definition

$f_n \in B_{n,m}$, injective. **The measure of feeble one-wayness** $M_F(f_n) = \frac{C(f_n^{-1})}{C(f_n)}$.

Definition

$\{f_n\}$ is **feebly one-way of order k** if $\liminf_{n\to\infty} C(f_n) = \infty$ and $\liminf_{n\to\infty} M_F(f_n) = k$, with $k \in (1, \infty]$.

Hiltgen's function of order 3/2

$$f_n((x_1, ...x_n)) = (y_1, ...y_n),$$

where

$$\begin{aligned} y_i &= x_i \oplus x_{i+1} & 1 \le i < n \\ y_i &= x_1 \oplus x_{\lceil n/2 \rceil} \oplus x_n & i = n. \end{aligned}$$

Hiltgen's function of order 3/2

$$f_n((x_1, \ldots x_n)) = (y_1, \ldots y_n),$$

where

$$\begin{aligned} y_i &= x_i \oplus x_{i+1} & 1 \leq i < n \\ y_i &= x_1 \oplus x_{\lceil n/2 \rceil} \oplus x_n & i = n. \end{aligned}$$

$$f_n^{-1}((y_1, \ldots y_n)) = (x_1, \ldots x_n),$$

where

$$\begin{aligned} x_i &= (y_1 \oplus \cdots \oplus y_{i-1}) \oplus (y_{\lceil n/2 \rceil} \oplus \cdots \oplus y_{n-1}) \oplus y_n & 1 \leq i \leq \lceil n/2 \rceil \\ x_i &= (y_1 \oplus \cdots \oplus y_{\lceil n/2 \rceil - 1}) \oplus (y_i \oplus \cdots \oplus y_{n-1}) \oplus y_n & \lceil n/2 \rceil \leq i \leq n. \end{aligned}$$

Hiltgen's function of order 3/2

$$f_n((x_1, ...x_n)) = (y_1, ...y_n),$$

where

$$\begin{aligned} y_i &= x_i \oplus x_{i+1} & 1 \leq i < n \\ y_i &= x_1 \oplus x_{\lceil n/2 \rceil} \oplus x_n & i = n. \end{aligned}$$

$$f_n^{-1}((y_1, ...y_n)) = (x_1, ...x_n),$$

where

$$\begin{aligned} x_i &= (y_1 \oplus \cdots \oplus y_{i-1}) \oplus (y_{\lceil n/2 \rceil} \oplus \cdots \oplus y_{n-1}) \oplus y_n & 1 \leq i \leq \lceil n/2 \rceil \\ x_i &= (y_1 \oplus \cdots \oplus y_{\lceil n/2 \rceil - 1}) \oplus (y_i \oplus \cdots \oplus y_{n-1}) \oplus y_n & \lceil n/2 \rceil \leq i \leq n. \end{aligned}$$

Theorem

For all $n > 5$, the functions f_n satisfy $C(f_n) = n + 1$ and $C(f_n^{-1}) = \lfloor \frac{3}{2}(n-1) \rfloor$.

Hiltgen's function of order 3/2

$$f_n((x_1, \ldots x_n)) = (y_1, \ldots y_n),$$

where

$$\begin{aligned} y_i &= x_i \oplus x_{i+1} & 1 \le i < n \\ y_i &= x_1 \oplus x_{\lceil n/2 \rceil} \oplus x_n & i = n. \end{aligned}$$

$$f_n^{-1}((y_1, \ldots y_n)) = (x_1, \ldots x_n),$$

where

$$\begin{aligned} x_i &= (y_1 \oplus \cdots \oplus y_{i-1}) \oplus (y_{\lceil n/2 \rceil} \oplus \cdots \oplus y_{n-1}) \oplus y_n & 1 \le i \le \lceil n/2 \rceil \\ x_i &= (y_1 \oplus \cdots \oplus y_{\lceil n/2 \rceil - 1}) \oplus (y_i \oplus \cdots \oplus y_{n-1}) \oplus y_n & \lceil n/2 \rceil \le i \le n. \end{aligned}$$

Theorem

For all $n > 5$, the functions f_n satisfy $C(f_n) = n + 1$ and $C(f_n^{-1}) = \lfloor \frac{3}{2}(n-1) \rfloor$.

Corollary

$\{f_n\}$ is feebly one-way of order $3/2$.

Methods

1. Gate elimination.
2. Lower bounds (Lamagna and Savage).

Theorem

If $f \in B_n$ depends non-idly on each of its n variables, then

$$C(f) \geq n - 1.$$

Theorem

Let $f = \{f^{(0)}, \ldots, f^{(m)}\} \in B_{n,m}$. If the m component functions $f^{(i)}$ are pairwise different and if they satisfy $C(f^{(i)}) \geq c \geq 1$, then

$$C(f) \geq c + m - 1.$$

Hiltgen's function of order 3/2

Proof.

1. $C(f_n) \leq n + 1$.

Hiltgen's function of order 3/2

Proof.

1. $C(f_n) \leq n + 1$.
2. $C(f_n) \geq n + 1$.

Hiltgen's function of order 3/2

Proof.

1. $C(f_n) \leq n + 1$.
2. $C(f_n) \geq n + 1$.
   1. Consider $S_1 = \{x_1, x_{\lceil n/2 \rceil}, x_n\}$, $S_2 = \{x_1, \ldots, x_n\} \setminus S_1$.

Hiltgen's function of order 3/2

Proof.

1. $C(f_n) \leq n + 1$.
2. $C(f_n) \geq n + 1$.
   1. Consider $S_1 = \{x_1, x_{\lceil n/2 \rceil}, x_n\}$, $S_2 = \{x_1, \ldots, x_n\} \setminus S_1$.
   2. Set $x_i = 0 \quad \forall x_i \in S_2$. We eliminate at least $n - 1$ gates.

Hiltgen's function of order 3/2

Proof.

1. $C(f_n) \leq n+1$.
2. $C(f_n) \geq n+1$.
    1. Consider $S_1 = \{x_1, x_{\lceil n/2 \rceil}, x_n\}$, $S_2 = \{x_1, \ldots, x_n\} \setminus S_1$.
    2. Set $x_i = 0 \quad \forall x_i \in S_2$. We eliminate at least $n-1$ gates.
    3. $C(y_n) = 2$.

Hiltgen's function of order 3/2

Proof.

1. $C(f_n) \leq n + 1$.
2. $C(f_n) \geq n + 1$.
   1. Consider $S_1 = \{x_1, x_{\lceil n/2 \rceil}, x_n\}$, $S_2 = \{x_1, \ldots, x_n\} \setminus S_1$.
   2. Set $x_i = 0 \quad \forall x_i \in S_2$. We eliminate at least $n - 1$ gates.
   3. $C(y_n) = 2$.
3. $C(f_n^{-1}) = \lfloor \frac{3}{2}(n - 1) \rfloor$.

Hiltgen's function of order 3/2

Proof.

1. $C(f_n) \leq n + 1$.
2. $C(f_n) \geq n + 1$.
    1. Consider $S_1 = \{x_1, x_{\lceil n/2 \rceil}, x_n\}$, $S_2 = \{x_1, \ldots, x_n\} \setminus S_1$.
    2. Set $x_i = 0 \quad \forall x_i \in S_2$. We eliminate at least $n - 1$ gates.
    3. $C(y_n) = 2$.
3. $C(f_n^{-1}) = \lfloor \frac{3}{2}(n-1) \rfloor$.
    1. $C(x_i) \geq \lceil n/2 \rceil - 1$.

Hiltgen's function of order 3/2

Proof.

1. $C(f_n) \leq n + 1$.
2. $C(f_n) \geq n + 1$.
   1. Consider $S_1 = \{x_1, x_{\lceil n/2 \rceil}, x_n\}$, $S_2 = \{x_1, \ldots, x_n\} \setminus S_1$.
   2. Set $x_i = 0 \quad \forall x_i \in S_2$. We eliminate at least $n - 1$ gates.
   3. $C(y_n) = 2$.
3. $C(f_n^{-1}) = \lfloor \frac{3}{2}(n - 1) \rfloor$.
   1. $C(x_i) \geq \lceil n/2 \rceil - 1$.
   2. $C(f_n^{-1}) \geq (\lceil n/2 \rceil - 1) + n - 1 = \lfloor \frac{3}{2}(n - 1) \rfloor$.

Hiltgen's function of order 3/2

Proof.

1. $C(f_n) \leq n + 1$.
2. $C(f_n) \geq n + 1$.
   1. Consider $S_1 = \{x_1, x_{\lceil n/2 \rceil}, x_n\}$, $S_2 = \{x_1, \ldots, x_n\} \setminus S_1$.
   2. Set $x_i = 0 \quad \forall x_i \in S_2$. We eliminate at least $n - 1$ gates.
   3. $C(y_n) = 2$.
3. $C(f_n^{-1}) = \lfloor \frac{3}{2}(n-1) \rfloor$.
   1. $C(x_i) \geq \lceil n/2 \rceil - 1$.
   2. $C(f_n^{-1}) \geq (\lceil n/2 \rceil - 1) + n - 1 = \lfloor \frac{3}{2}(n-1) \rfloor$.
   3. $x_i = y_i \oplus x_{i+1}, i \neq n \Longrightarrow C(f_n^{-1}) \leq \lfloor \frac{3}{2}(n-1) \rfloor$.

□

Hiltgen's function of order 3/2

Proof.

1. $C(f_n) \leq n + 1$.
2. $C(f_n) \geq n + 1$.
   1. Consider $S_1 = \{x_1, x_{\lceil n/2 \rceil}, x_n\}$, $S_2 = \{x_1, \ldots, x_n\} \setminus S_1$.
   2. Set $x_i = 0 \quad \forall x_i \in S_2$. We eliminate at least $n - 1$ gates.
   3. $C(y_n) = 2$.
3. $C(f_n^{-1}) = \lfloor \frac{3}{2}(n-1) \rfloor$.
   1. $C(x_i) \geq \lceil n/2 \rceil - 1$.
   2. $C(f_n^{-1}) \geq (\lceil n/2 \rceil - 1) + n - 1 = \lfloor \frac{3}{2}(n-1) \rfloor$.
   3. $x_i = y_i \oplus x_{i+1}, i \neq n \Longrightarrow C(f_n^{-1}) \leq \lfloor \frac{3}{2}(n-1) \rfloor$.

□

Remark

Hiltgen improved this family of permutations and got order 2.

Perspectives

- Linear constructions: $\leq n-1$ gates per one bit of output.
- f is linear $\implies$ f^{-1} is also linear.

Perspectives

- Linear constructions: $\leq n - 1$ gates per one bit of output.
- f is linear $\implies$ f^{-1} is also linear.
- **Nonlinear constructions are necessary!**

Non-linear function of order 2

$$
\begin{aligned}
y_1 &= (x_1 \oplus x_2)x_n \oplus x_{n-1} \\
y_2 &= (x_1 \oplus x_2)x_n \oplus x_2 \\
y_3 &= x_1 \oplus x_3 \\
y_4 &= x_3 \oplus x_4 \\
&\dots \\
y_{n-1} &= x_{n-2} \oplus x_{n-1} \\
y_n &= x_n
\end{aligned}
$$

Non-linear function of order 2

$$
\begin{aligned}
y_1 &= (x_1 \oplus x_2)x_n \oplus x_{n-1} \\
y_2 &= (x_1 \oplus x_2)x_n \oplus x_2 \\
y_3 &= x_1 \oplus x_3 \\
y_4 &= x_3 \oplus x_4 \\
&\dots \\
y_{n-1} &= x_{n-2} \oplus x_{n-1} \\
y_n &= x_n
\end{aligned}
$$

$$
\begin{aligned}
x_n &= y_n \\
x_2 &= (y_1 \oplus \dots \oplus y_{n-1})y_n \oplus y_2 \\
x_{n-1} &= (y_1 \oplus \dots \oplus y_{n-1})y_n \oplus y_1 \\
x_{n-2} &= (y_1 \oplus \dots \oplus y_{n-1})y_n \oplus y_1 \oplus y_{n-1} \\
x_{n-3} &= (y_1 \oplus \dots \oplus y_{n-1})y_n \oplus y_1 \oplus y_{n-1} \oplus y_{n-2} \\
&\dots \\
x_3 &= (y_1 \oplus \dots \oplus y_{n-1})y_n \oplus y_1 \oplus y_{n-1} \oplus \dots \oplus y_4 \\
x_1 &= (y_1 \oplus \dots \oplus y_{n-1})y_n \oplus y_1 \oplus y_{n-1} \oplus \dots \oplus y_3
\end{aligned}
$$

Non-linear function of order 2

Theorem

$\{f_n\}$ *is feebly one-way of order* 2.

Non-linear function of order 2

Theorem

$\{f_n\}$ *is feebly one-way of order* 2.

Proof.

1. $n - 1 \leq C(f_n) \leq n + 1$.

Non-linear function of order 2

Theorem

$\{f_n\}$ *is feebly one-way of order* 2.

Proof.

1. $n - 1 \leq C(f_n) \leq n + 1$.
2. $2n - 3 \leq C(f_n^{-1}) \leq 2n - 2$.

Non-linear function of order 2

Theorem

$\{f_n\}$ *is feebly one-way of order* 2.

Proof.

1. $n - 1 \leq C(f_n) \leq n + 1$.
2. $2n - 3 \leq C(f_n^{-1}) \leq 2n - 2$.
3. $\frac{2n-3}{n+1} \leq M_F(f_n) \leq \frac{2n-2}{n-1}$.

□

Average case complexity

Notation

$C_\alpha(f)$ – the minimal size of a circuit that correctly computes a function $f \in B_{n,m}$ on more than αn of its inputs ($\alpha \in (0, 1)$).

Average case complexity

Notation

$C_\alpha(f)$ – the minimal size of a circuit that correctly computes a function $f \in B_{n,m}$ on more than αn of its inputs ($\alpha \in (0,1)$).

Theorem

$C_{3/4}(f_n^{-1}) \geq 2n - 4$.

Average case complexity

Notation

$C_\alpha(f)$ – the minimal size of a circuit that correctly computes a function $f \in B_{n,m}$ on more than αn of its inputs ($\alpha \in (0,1)$).

Theorem

$C_{3/4}(f_n^{-1}) \geq 2n - 4$.

Proof (Idea)

1. Consider optimal circuit for f_n^{-1}
2. Step: substitute in place of y_i ($i \neq n$) value from $\{0, 1, y_n, y_n \oplus 1\}$ that eliminates at least 2 gates.
3. Repeat $n - 2$ times.

Average case complexity

Notation

$C_\alpha(f)$ – the minimal size of a circuit that correctly computes a function $f \in B_{n,m}$ on more than αn of its inputs ($\alpha \in (0,1)$).

Theorem

$C_{3/4}(f_n^{-1}) \geq 2n - 4$.

Proof (Idea)

1. Consider optimal circuit for f_n^{-1}
2. Step: substitute in place of y_i ($i \neq n$) value from $\{0, 1, y_n, y_n \oplus 1\}$ that eliminates at least 2 gates.
3. Repeat $n - 2$ times.

Lemma (unformally)

We can repeat our step $n - 2$ times.

Average case complexity

Lemma (formalization)

In circuit, which computes $f_n^{-1}|_{y_{i_1}=a_1,\ldots,y_{i_l}=a_l}$ with $l \leq n-3$, $n \notin \{i_1,\ldots,i_l\}$ and $\forall k \in [1..l]$ $a_{i_k} \in \{0,1,y_n,y_n \oplus 1\}$ on more than $\frac{3}{4}$ inputs, one can substitute in place of y_i ($i \neq n$) value from $\{0,1,y_n,y_n \oplus 1\}$ that eliminates at least 2 gates and obtained circuit computes f_n^{-1} on more than $\frac{3}{4}$ residuary inputs.

Average case complexity

Lemma (formalization)

In circuit, which computes $f_n^{-1}|_{y_{i_1}=a_1,\ldots,y_{i_l}=a_l}$ with $l \le n-3$, $n \notin \{i_1,\ldots,i_l\}$ and $\forall k \in [1..l]\ a_{i_k} \in \{0,1,y_n,y_n \oplus 1\}$ on more than $\frac{3}{4}$ inputs, one can substitute in place of y_i ($i \ne n$) value from $\{0,1,y_n,y_n \oplus 1\}$ that eliminates at least 2 gates and obtained circuit computes f_n^{-1} on more than $\frac{3}{4}$ residuary inputs.

Proof.

Consider topmost gate g. Let y_i and y_j be inputs.

1. y_i enters some other gate and $i \ne n$.
2. Neither y_i nor y_j enters any other gate and $i, j \ne n$.
3. $j = n$, y_i doesn't enter any other gate and g is non-linear.
4. $j = n$, y_i doesn't enter any other gate and g is linear.

Average case complexity

Lemma (formalization)

In circuit, which computes $f_n^{-1}|_{y_{i_1}=a_1,\ldots,y_{i_l}=a_l}$ with $l \leq n-3$, $n \notin \{i_1, \ldots, i_l\}$ and $\forall k \in [1..l]$ $a_{i_k} \in \{0, 1, y_n, y_n \oplus 1\}$ on more than $\frac{3}{4}$ inputs, one can substitute in place of y_i ($i \neq n$) value from $\{0, 1, y_n, y_n \oplus 1\}$ that eliminates at least 2 gates and obtained circuit computes f_n^{-1} on more than $\frac{3}{4}$ residuary inputs.

Proof.

Consider topmost gate g. Let y_i and y_j be inputs.

1. y_i enters some other gate and $i \neq n$.
2. Neither y_i nor y_j enters any other gate and $i, j \neq n$.
3. $j = n$, y_i doesn't enter any other gate and g is non-linear.
4. $j = n$, y_i doesn't enter any other gate and g is linear.
   Assume g is output h_k. Then
   1. $x_k|_{y_n=1} = y_l \oplus \ldots$ or $x_k|_{y_n=0} = y_l \oplus \ldots$.
   2. $x_k = y_n$.

Average case complexity

Lemma (formalization)

In circuit, which computes $f_n^{-1}|_{y_{i_1}=a_1,\dots,y_{i_l}=a_l}$ with $l \le n-3$, $n \notin \{i_1,\dots,i_l\}$ and $\forall k \in [1..l]$ $a_{i_k} \in \{0,1,y_n,y_n \oplus 1\}$ on more than $\frac{3}{4}$ inputs, one can substitute in place of y_i ($i \neq n$) value from $\{0,1,y_n,y_n \oplus 1\}$ that eliminates at least 2 gates and obtained circuit computes f_n^{-1} on more than $\frac{3}{4}$ residuary inputs.

Proof.

Consider topmost gate g. Let y_i and y_j be inputs.

1. y_i enters some other gate and $i \neq n$.
2. Neither y_i nor y_j enters any other gate and $i, j \neq n$.
3. $j = n$, y_i doesn't enter any other gate and g is non-linear.
4. $j = n$, y_i doesn't enter any other gate and g is linear.
   Assume g is output h_k. Then
   1. $x_k|_{y_n=1} = y_l \oplus \dots$ or $x_k|_{y_n=0} = y_l \oplus \dots$.
   2. $x_k = y_n$.

   g has children. Substitute $y_i = y_n$ or $y_i = y_n \oplus 1$.

□

Hardness amplification

Let $H(x^{(1)}, \ldots, x^{(m)}) = (f_n(x^{(1)}), \ldots, f(x^{(m)}))$,
where $x^{(i)} = (x_{i_1}, \ldots, x_{i_n})$.

Theorem

$p(m)$ – *any function.*
$C_{1/p(m)}(H^{-1}) \geq (2n-4)(m - \log_{4/3} p(m))$.

Further research

1. to improve the order of security;
2. to devise other feebly secure cryptographic primitives.

Further research

1. to improve the order of security;
2. to devise other feebly secure cryptographic primitives.

   Known results:

   1. Linear feebly trapdoor construction (based on Hiltgen's function of order $3/2$) of order $\frac{25}{22}$;
   2. Quadratic feebly trapdoor construction (based on function of order 2) of order $\frac{7}{5}$.