Cryptographic Hash Function
EDON-R

Presented by
Prof. Danilo Gligoroski

Department of Telematics
Faculty of Information Technology, Mathematics and Electrical Engineering
Norwegian University of Science and Technology - NTNU, NORWAY
Outline

- Short history of EDON-R
- Specific design characteristics
- Known attacks on EDON-R
- Are there any one-way bijections embedded in EDON-R?
- SW/HW performance and memory requirements
Short history of EDON-R

- Theoretical principles of EDON-R were described at the Second NIST Hash Workshop – 2006 in the presentation: *Edon-R Family of Cryptographic Hash Functions*
  - No concrete realization
Short history of EDON-R

- Theoretical principles of EDON-R were described at the Second NIST Hash Workshop – 2006 in the presentation: **Edon-R Family of Cryptographic Hash Functions**
  - No concrete realization

  - **Big acknowledgement** for Søren Steffen Thomsen, giving me comments about zero being a fixed point in that realization
Short history of EDON-R

- Additionally, the following contributors joined the EDON-R (SHA-3) team:
  - Rune Steinsmo Ødegård – Investigating the mathematical properties of defined quasigroups
  - Marija Mihova – Investigating the differential properties in EDON-R operations
  - Svein Johan Knapskog (general comments and suggestions for improvements, proofreading)
  - Ljupco Kocarev (general comments and suggestions for improvements, proofreading)
  - Aleš Drápal (Theory of quasigroups and suggestions for improvements)
  - Vlastimil Klima (cryptanalysis and suggestions for improvements)
**Specific design characteristics for EDON-R**

**Algorithm: EDON-R**

**Input:** Message $M$ of length $t$ bits, and the message digest size $n$.

**Output:** A message digest $\text{Hash}$, that is long $n$ bits.

1. **Preprocessing**
   - (a) Pad the message $M$.
   - (b) Parse the padded message into $N$, $t$-bit message blocks, $M^{(1)}$, $M^{(2)}$, ..., $M^{(N)}$.
   - (c) Set the initial value of the double pipe $P^{(0)}$.

2. **Hash computation**
   
   For $i = 1$ to $N$
   
   $P^{(i)} = R(M^{(i-1)}, P^{(i-1)})$;

3. **Hash** = Take $n$ Least Significant Bits($P^{(N)}$).

---

[Diagram showing the algorithm steps with equations and values for $M^{(1)}$, $M^{(2)}$, ..., $M^{(N)}$, $X^{(1)}$, $X^{(2)}$, ..., $X^{(N)}$, and $P^{(0)}$, $P^{(1)}$, $P^{(2)}$, ..., $P^{(N)}$.]

---

**NTNU Innovation and Creativity**

[Website link: www.ntnu.no]
Specific design characteristics for EDON-R

1. Preprocessing
   (a) Pad the message $M$.
   (b) Parse the padded message into $N$, $m$-bit message blocks, $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$.
   (c) Set the initial value of the double pipe $P^{(0)}$.

2. Hash computation
   For $i = 1$ to $N$
   $P^{(i)} = \mathcal{R}(P^{(i-1)}, M^{(i)})$.

3. $Hash = \text{Take}_n\_\text{Least}_\text{Significant}_\text{Bits}(P^{(N)})$.
Specific design characteristics for EDON-R

Algorithm: EDON-R

Input: Message $M$ of length $t$ bits, and the message digest size $n$.
Output: A message digest Hash, that is long $n$ bits.

1. Preprocessing
   (a) Pad the message $M$.
   (b) Parse the padded message into $N$, $n$-bit message blocks, $M^{(1)}$, $M^{(2)}$, ..., $M^{(N)}$.
   (c) Set the initial value of the double pipe $P^{(0)}$.

2. Hash computation
   For $i = 1$ to $N$
   \[
   P^{(i)} = \mathcal{R}(P^{(i-1)}, M^{(i)});
   \]

3. $Hash = Take_{n\text{-Least\text{-}Significant\text{-}Bits}}(P^{(N)})$.  

www.ntnu.no

Specific design characteristics for EDON-R

Algorithm: EDON-R

1. Preprocessing
   (a) Pad the message $M$.
   (b) Parse the padded message into $N$, $m$-bit message blocks, $M^{(1)}$, $M^{(2)}$, ..., $M^{(N)}$.
   (c) Set the initial value of the double pipe $P^{(0)}$.

2. Hash computation

   For $i = 1$ to $N$
   
   $P^{(i)} = \mathcal{R}(P^{(i-1)}, M^{(i)})$;

3. $Hash = \text{Take}_n \text{Least Significan Bits}(P^{(N)})$.

$9$


www.ntnu.no
Specific design characteristics for EDON-R

Algorithm: EDON-R

Input: Message $M$ of length $t$ bits, and the message digest size $n$.

Output: A message digest $Hash$, that is long $n$ bits.

1. Preprocessing
   (a) Pad the message $M$.
   (b) Parse the padded message into $N$, $m$-bit message blocks, $M^{(1)}$, $M^{(2)}$, $\ldots$, $M^{(N)}$.
   (c) Set the initial value of the double pipe $P^{(0)}$.

2. Hash computation
   
   For $i = 1$ to $N$
   
   $P^{(i)} = R(P^{(i-1)}, M^{(i)})$

3. $Hash = Take_{n\text{-Least\_Significant\_Bits}}(P^{(N)})$. 

Specific design characteristics for EDON-R

Algorithm: EDON-R

Input: A message digest hash, that is long \( n \) bits.

Output: A message digest hash, that is long \( n \) bits.

1. preprocessing
   (a) Pad the message \( M \).
   (b) Parse the padded message into \( N \), \( n \)-bit message blocks, \( M^{(1)}, M^{(2)}, \ldots, M^{(N)} \).
   (c) Set the initial value of the double pipe \( P^{(0)} \).

2. Hash computation
   For \( i = 1 \) to \( N \)
   \[
   R^{(i)} = R(P^{(i-1)}, M^{(i)});
   \]

3. Hash = Take \( n \)-Least Significant Bits \( P^{(N)} \).
Specific design characteristics for EDON-R

Algorithm: EDON-R

Input: Message $M$ of length $t$ bits, and the message digest size $n$.

Output: A message digest Hash, that is long $n$ bits.

1. Preprocessing
   (a) Pad the message $M$.
   (b) Parse the padded message into $N$, $n$-bit message blocks, $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$.
   (c) Set the initial value of the double pipe $P^{(0)}$.

2. Hash computation
   For $i = 1$ to $N$
   
   $P^{(i)} = R(P^{(i-1)}, M^{(i)})$;

3. $Hash = \text{Take}_n\text{Least}_\text{Significant}_\text{Bits}(P^{(N)})$.

Function $R(C_0, C_1, A_0, A_1)$ is defined by quasigroup operations.
Specific design characteristics for EDON-R

Quasigroup operations are defined on 256-bit or 512-bit operands.

\[ X \ast Y \]
Specific design characteristics for EDON-R

Quasigroup operations are defined on 256-bit or 512-bit operands.

\[
(X_0, X_1, \ldots, X_7) \ast (Y_0, Y_1, \ldots, Y_7)
\]

32-bit or 64-bit variables
Specific design characteristics for EDON-R

Quasigroup operations are defined on 256-bit or 512-bit operands.

\[ (X_0, X_1, \ldots, X_7) \star (Y_0, Y_1, \ldots, Y_7) \]

Operations:
1. Additions modulo \(2^{32}\) or modulo \(2^{64}\)
2. Left rotations of 32-bit or 64-bit words
3. Bitwise XOR operations of 32-bit or 64-bit words
### Specific design characteristics for EDON-R

#### Quasigroup operation of order $2^{256}$

**Input:** $X = (X_0, X_1, \ldots, X_7)$ and $Y = (Y_0, Y_1, \ldots, Y_7)$

where $X_i$ and $Y_i$ are 32–bit variables.

**Output:** $Z = (Z_0, Z_1, \ldots, Z_7)$ where $Z_i$ are 32–bit variables.

**Temporary 32–bit variables:** $T_0, \ldots, T_{15}$

1. 

   \[
   \begin{align*}
   T_0 & \leftarrow \text{ROTL}^0(0xAAAAA) + X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6; \\
   T_1 & \leftarrow \text{ROTL}^4(X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6); \\
   T_2 & \leftarrow \text{ROTL}^8(X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6); \\
   T_3 & \leftarrow \text{ROTL}^{12}(X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6); \\
   T_4 & \leftarrow \text{ROTL}^{16}(X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6); \\
   T_5 & \leftarrow \text{ROTL}^{20}(X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6); \\
   T_6 & \leftarrow \text{ROTL}^{24}(X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6); \\
   T_7 & \leftarrow \text{ROTL}^{28}(X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6); \\
   T_8 & \leftarrow T_3 \oplus T_5 \oplus T_6; \\
   T_9 & \leftarrow T_2 \oplus T_5 \oplus T_6; \\
   T_{10} & \leftarrow T_2 \oplus T_5 \oplus T_6; \\
   T_{11} & \leftarrow T_0 \oplus T_1 \oplus T_5; \\
   T_{12} & \leftarrow T_0 \oplus T_4 \oplus T_7; \\
   T_{13} & \leftarrow T_1 \oplus T_6 \oplus T_7; \\
   T_{14} & \leftarrow T_2 \oplus T_3 \oplus T_4; \\
   T_{15} & \leftarrow T_0 \oplus T_1 \oplus T_7;
   \end{align*}
   \]

2. 

   \[
   \begin{align*}
   T_0 & \leftarrow \text{ROTL}^0(0x55555555) + Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6; \\
   T_1 & \leftarrow \text{ROTL}^5(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6); \\
   T_2 & \leftarrow \text{ROTL}^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6); \\
   T_3 & \leftarrow \text{ROTL}^{11}(Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7); \\
   T_4 & \leftarrow \text{ROTL}^{15}(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6); \\
   T_5 & \leftarrow \text{ROTL}^{20}(Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7); \\
   T_6 & \leftarrow \text{ROTL}^{24}(Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7); \\
   T_7 & \leftarrow \text{ROTL}^{28}(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7); \\
   T_8 & \leftarrow T_3 \oplus T_4 \oplus T_6; \\
   T_9 & \leftarrow T_2 \oplus T_5 \oplus T_7; \\
   T_{10} & \leftarrow T_4 \oplus T_6 \oplus T_7; \\
   T_{11} & \leftarrow T_0 \oplus T_1 \oplus T_5; \\
   T_{12} & \leftarrow T_1 \oplus T_6 \oplus T_7; \\
   T_{13} & \leftarrow T_2 \oplus T_3 \oplus T_4; \\
   T_{14} & \leftarrow T_0 \oplus T_1 \oplus T_7; \\
   T_{15} & \leftarrow T_1 \oplus T_2 \oplus T_3; \\
   Z_5 & \leftarrow T_{11} \oplus T_3 \oplus T_4 \oplus T_6; \\
   Z_6 & \leftarrow T_9 \oplus T_2 \oplus T_5 \oplus T_7; \\
   Z_7 & \leftarrow T_{10} \oplus T_4 \oplus T_6 \oplus T_7; \\
   Z_0 & \leftarrow T_{11} \oplus T_0 \oplus T_1 \oplus T_3; \\
   Z_1 & \leftarrow T_{12} \oplus T_2 \oplus T_6 \oplus T_7; \\
   Z_2 & \leftarrow T_{13} \oplus T_0 \oplus T_1 \oplus T_3; \\
   Z_3 & \leftarrow T_{14} \oplus T_0 \oplus T_3 \oplus T_4; \\
   Z_4 & \leftarrow T_{15} \oplus T_1 \oplus T_2 \oplus T_3;
   \end{align*}
   \]

3. 

   \[
   X \ast Y \equiv \pi_1(\pi_2(X) + 8\pi_3(Y))
   \]
Specific design characteristics for EDON-R

Quasigroup operation of order $2^{256}$

| Input: $X = (X_0, X_1, \ldots, X_7)$ and $Y = (Y_0, Y_1, \ldots, Y_7)$ |
| where $X_i$ and $Y_i$ are 32-bit variables. |
| Output: $Z = (Z_0, Z_1, \ldots, Z_7)$ where $Z_i$ are 32-bit variables. |
| Temporary 32-bit variables: $T_0, \ldots, T_{15}$. |

<table>
<thead>
<tr>
<th>1.</th>
<th>2.</th>
<th>3.</th>
<th>4.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_0 \leftarrow \text{ROTL}^0(0xAAAAAAAA}$</td>
<td>$T_0 \leftarrow \text{ROTL}^0(0x55555555)$</td>
<td>$T_0 \leftarrow \text{ROTL}^0(0x)$</td>
<td>$T_0 \leftarrow \text{ROTL}^0(0x)$</td>
</tr>
<tr>
<td>$T_1 \leftarrow \text{ROTL}^1(0x)$</td>
<td>$T_1 \leftarrow \text{ROTL}^1(0x)$</td>
<td>$T_1 \leftarrow \text{ROTL}^1(0x)$</td>
<td>$T_1 \leftarrow \text{ROTL}^1(0x)$</td>
</tr>
<tr>
<td>$T_2 \leftarrow \text{ROTL}^2(0x)$</td>
<td>$T_2 \leftarrow \text{ROTL}^2(0x)$</td>
<td>$T_2 \leftarrow \text{ROTL}^2(0x)$</td>
<td>$T_2 \leftarrow \text{ROTL}^2(0x)$</td>
</tr>
<tr>
<td>$T_3 \leftarrow \text{ROTL}^3(0x)$</td>
<td>$T_3 \leftarrow \text{ROTL}^3(0x)$</td>
<td>$T_3 \leftarrow \text{ROTL}^3(0x)$</td>
<td>$T_3 \leftarrow \text{ROTL}^3(0x)$</td>
</tr>
<tr>
<td>$T_4 \leftarrow \text{ROTL}^4(0x)$</td>
<td>$T_4 \leftarrow \text{ROTL}^4(0x)$</td>
<td>$T_4 \leftarrow \text{ROTL}^4(0x)$</td>
<td>$T_4 \leftarrow \text{ROTL}^4(0x)$</td>
</tr>
<tr>
<td>$T_5 \leftarrow \text{ROTL}^5(0x)$</td>
<td>$T_5 \leftarrow \text{ROTL}^5(0x)$</td>
<td>$T_5 \leftarrow \text{ROTL}^5(0x)$</td>
<td>$T_5 \leftarrow \text{ROTL}^5(0x)$</td>
</tr>
<tr>
<td>$T_6 \leftarrow \text{ROTL}^6(0x)$</td>
<td>$T_6 \leftarrow \text{ROTL}^6(0x)$</td>
<td>$T_6 \leftarrow \text{ROTL}^6(0x)$</td>
<td>$T_6 \leftarrow \text{ROTL}^6(0x)$</td>
</tr>
<tr>
<td>$T_7 \leftarrow \text{ROTL}^7(0x)$</td>
<td>$T_7 \leftarrow \text{ROTL}^7(0x)$</td>
<td>$T_7 \leftarrow \text{ROTL}^7(0x)$</td>
<td>$T_7 \leftarrow \text{ROTL}^7(0x)$</td>
</tr>
<tr>
<td>$T_8 \leftarrow T_3 \oplus T_5 \oplus T_6$</td>
<td>$T_8 \leftarrow T_3 \oplus T_5 \oplus T_6$</td>
<td>$T_8 \leftarrow T_3 \oplus T_5 \oplus T_6$</td>
<td>$T_8 \leftarrow T_3 \oplus T_5 \oplus T_6$</td>
</tr>
<tr>
<td>$T_9 \leftarrow T_3 \oplus T_5 \oplus T_6$</td>
<td>$T_9 \leftarrow T_3 \oplus T_5 \oplus T_6$</td>
<td>$T_9 \leftarrow T_3 \oplus T_5 \oplus T_6$</td>
<td>$T_9 \leftarrow T_3 \oplus T_5 \oplus T_6$</td>
</tr>
<tr>
<td>$T_{10} \leftarrow T_7 \oplus T_9 \oplus T_{10}$</td>
<td>$T_{10} \leftarrow T_7 \oplus T_9 \oplus T_{10}$</td>
<td>$T_{10} \leftarrow T_7 \oplus T_9 \oplus T_{10}$</td>
<td>$T_{10} \leftarrow T_7 \oplus T_9 \oplus T_{10}$</td>
</tr>
<tr>
<td>$T_{11} \leftarrow T_7 \oplus T_9 \oplus T_{10}$</td>
<td>$T_{11} \leftarrow T_7 \oplus T_9 \oplus T_{10}$</td>
<td>$T_{11} \leftarrow T_7 \oplus T_9 \oplus T_{10}$</td>
<td>$T_{11} \leftarrow T_7 \oplus T_9 \oplus T_{10}$</td>
</tr>
<tr>
<td>$T_{12} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
<td>$T_{12} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
<td>$T_{12} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
<td>$T_{12} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
</tr>
<tr>
<td>$T_{13} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
<td>$T_{13} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
<td>$T_{13} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
<td>$T_{13} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
</tr>
<tr>
<td>$T_{14} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
<td>$T_{14} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
<td>$T_{14} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
<td>$T_{14} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
</tr>
<tr>
<td>$T_{15} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
<td>$T_{15} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
<td>$T_{15} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
<td>$T_{15} \leftarrow T_9 \oplus T_{10} \oplus T_{12}$</td>
</tr>
</tbody>
</table>

Simple re-indexing (no computational costs)
Specific design characteristics for EDON-R

Quasigroup operation of order $2^{256}$

Input: $X = (X_0, X_1, \ldots, X_7)$ and $Y = (Y_0, Y_1, \ldots, Y_7)$

where $X_i$ and $Y_i$ are 32-bit variables.

Output: $Z = (Z_0, Z_1, \ldots, Z_7)$ where $Z_i$ are 32-bit variables.

Temporary 32-bit variables: $T_0, \ldots, T_{15}$.

$$X \ast Y \equiv \pi_1(\pi_2(X) + 8 \pi_3(Y))$$

$$L_1 = \begin{bmatrix}
0 & 7 & 1 & 3 & 2 & 4 & 6 & 5 \\
4 & 1 & 7 & 6 & 3 & 0 & 5 & 2 \\
7 & 0 & 4 & 2 & 5 & 3 & 1 & 6 \\
1 & 4 & 0 & 5 & 6 & 2 & 7 & 3 \\
2 & 3 & 6 & 7 & 1 & 5 & 0 & 4 \\
5 & 2 & 3 & 1 & 7 & 6 & 4 & 0 \\
3 & 6 & 5 & 0 & 4 & 7 & 2 & 1 \\
6 & 5 & 2 & 4 & 0 & 1 & 3 & 7
\end{bmatrix}$$
Specific design characteristics for EDON-R

Quasigroup operation of order $2^{256}$

Input: $X = (X_0, X_1, \ldots, X_7)$ and $Y = (Y_0, Y_1, \ldots, Y_7)$

where $X_i$ and $Y_i$ are 32-bit variables.

Output: $Z = (Z_0, Z_1, \ldots, Z_7)$ where $Z_i$ are 32-bit variables.

Temporary 32-bit variables: $T_0, \ldots, T_{15}$.

1. $T_0 \leftarrow ROLT^0(0xAAAAAAA) + X_0 + X_1 + X_2 + X_4 + X_5$;
   $T_1 \leftarrow ROLT^4(X_0 + X_1 + X_3 + X_4 + X_5);
   T_2 \leftarrow ROLT^8(X_0 + X_1 + X_4 + X_5 + X_6);
   T_3 \leftarrow ROLT^{12}(X_0 + X_1 + X_4 + X_5 + X_7);
   T_4 \leftarrow ROLT^{16}(X_0 + X_2 + X_3 + X_4 + X_5);
   T_5 \leftarrow ROLT^{17}(X_0 + X_1 + X_3 + X_4 + X_5);
   T_6 \leftarrow ROLT^{20}(X_0 + X_1 + X_3 + X_4 + X_5);
   T_7 \leftarrow ROLT^{24}(X_0 + X_1 + X_3 + X_4 + X_5).

2. $T_8 \leftarrow T_3 \oplus T_5 \oplus T_6$;
   $T_9 \leftarrow T_2 \oplus T_3 \oplus T_5$;
   $T_{10} \leftarrow T_0 \oplus T_3 \oplus T_4$;
   $T_{11} \leftarrow T_0 \oplus T_4 \oplus T_7$;
   $T_{12} \leftarrow T_0 \oplus T_4 \oplus T_7$;
   $T_{13} \leftarrow T_1 \oplus T_6 \oplus T_4$;
   $T_{14} \leftarrow T_2 \oplus T_5 \oplus T_7$;
   $T_{15} \leftarrow T_1 \oplus T_7 \oplus T_5$.

3. $T_6 \leftarrow ROLT^0(0x55555555) + Y_0 + Y_1 + Y_2 + Y_5 + Y_7$;
   $T_7 \leftarrow ROLT^{5}(Y_0 + Y_1 + Y_2 + Y_3 + Y_5 + Y_6)$;
   $T_8 \leftarrow ROLT^{9}(Y_0 + Y_1 + Y_2 + Y_3 + Y_5 + Y_6)$;
   $T_9 \leftarrow ROLT^{11}(Y_0 + Y_1 + Y_2 + Y_3 + Y_5 + Y_6)$;
   $T_{10} \leftarrow ROLT^{15}(Y_0 + Y_1 + Y_2 + Y_3 + Y_5 + Y_6)$;
   $T_{11} \leftarrow ROLT^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);
   T_{12} \leftarrow ROLT^{24}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);
   T_{13} \leftarrow ROLT^{27}(Y_0 + Y_1 + Y_2 + Y_3 + Y_5 + Y_6 + Y_7).

4. $Z_5 \leftarrow T_{18} + (T_3 \oplus T_4 \oplus T_6)$;
   $Z_6 \leftarrow T_{19} + (T_2 \oplus T_5 \oplus T_7)$;
   $Z_7 \leftarrow T_{10} + (T_4 \oplus T_6 \oplus T_7)$;
   $Z_8 \leftarrow T_{11} + (T_0 \oplus T_1 \oplus T_3)$;
   $Z_9 \leftarrow T_{12} + (T_2 \oplus T_6 \oplus T_7)$;
   $Z_{10} \leftarrow T_{13} + (T_0 \oplus T_1 \oplus T_3)$;
   $Z_{11} \leftarrow T_{14} + (T_0 \oplus T_3 \oplus T_4)$;
   $Z_{12} \leftarrow T_{15} + (T_1 \oplus T_2 \oplus T_3)$.

$L_1 = \begin{bmatrix} 0 & 7 & 1 & 3 & 2 & 4 & 6 & 5 \\
4 & 1 & 7 & 6 & 3 & 0 & 5 & 2 \\
7 & 0 & 4 & 2 & 5 & 3 & 1 & 6 \\
1 & 4 & 0 & 5 & 6 & 2 & 7 & 3 \\
2 & 3 & 6 & 7 & 1 & 5 & 0 & 4 \end{bmatrix}$

Specific design characteristics for EDON-R

Quasigroup operation of order $2^{256}$

Input: $X = (X_0, X_1, \ldots, X_7)$ and $Y = (Y_0, Y_1, \ldots, Y_7)$
where $X_i$ and $Y_i$ are 32-bit variables.

Output: $Z = (Z_0, Z_1, \ldots, Z_7)$ where $Z_i$ are 32-bit variables.

Temporary 32-bit variables: $T_0, \ldots, T_{15}.$

\[
X \ast Y \equiv \pi_1(\pi_2(X) + 8 \pi_3(Y))
\]
### Specific design characteristics for EDON-R

**Quasigroup operation of order $2^{256}$**

- **Input:** $X = (X_0, X_1, \ldots, X_7)$ and $Y = (Y_0, Y_1, \ldots, Y_7)$
- where $X_i$ and $Y_i$ are 32-bit variables.

- **Output:** $Z = (Z_0, Z_1, \ldots, Z_7)$ where $Z_i$ are 32-bit variables.

**Temporary 32-bit variables:** $T_0, \ldots, T_{15}$.

1. $T_0 \leftarrow ROTL^0(0xAAAAAA) + X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6$
2. $T_1 \leftarrow \begin{array}{l} + \text{ ROTL}^4(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6) \\ \text{ ROTL}^8(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6) \\ \text{ ROTL}^{12}(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6) \\ \text{ ROTL}^{16}(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6) \\ \text{ ROTL}^{20}(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6) \\ \text{ ROTL}^{24}(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6) \\ \text{ ROTL}^{28}(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6) \end{array}$
3. $T_2 \leftarrow \begin{array}{l} + \text{ ROTL}^5(Z_0 + Z_1 + Z_2 + Z_3 + Z_4 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7) \\ \text{ ROTL}^{10}(Z_0 + Z_1 + Z_2 + Z_3 + Z_4 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7) \\ \text{ ROTL}^{15}(Z_0 + Z_1 + Z_2 + Z_3 + Z_4 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7) \\ \text{ ROTL}^{20}(Z_0 + Z_1 + Z_2 + Z_3 + Z_4 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7) \\ \text{ ROTL}^{25}(Z_0 + Z_1 + Z_2 + Z_3 + Z_4 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7) \\ \text{ ROTL}^{30}(Z_0 + Z_1 + Z_2 + Z_3 + Z_4 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7) \end{array}$

\[
X \ast Y \equiv \pi_1(\pi_2(X) + 8 \pi_3(Y))
\]

**Example:**

\[
L_1 = \begin{bmatrix} L_{1,1} \\ L_{1,2} \end{bmatrix}
\]

- $L_1 = \begin{bmatrix} 7 & 1 & 3 & 2 & 4 & 6 & 5 \\ 4 & 1 & 7 & 6 & 3 & 0 & 5 & 2 \\ 0 & 4 & 2 & 5 & 3 & 1 & 6 \\ 4 & 0 & 5 & 6 & 2 & 7 & 3 \\ 3 & 6 & 7 & 1 & 5 & 0 & 4 \\ 5 & 2 & 3 & 1 & 7 & 6 & 4 & 0 \\ 6 & 5 & 0 & 4 & 7 & 2 & 1 \\ 6 & 5 & 2 & 4 & 0 & 1 & 3 & 7 \end{bmatrix}
\]
Specific design characteristics for EDON-R

Quasigroup operation of order $2^{256}$

Input: $X = (X_0, X_1, \ldots, X_7)$ and $Y = (Y_0, Y_1, \ldots, Y_7)$

where $X_i$ and $Y_i$ are 32-bit variables.

Output: $Z = (Z_0, Z_1, \ldots, Z_7)$ where $Z_i$ are 32-bit variables.

Temporary 32-bit variables: $T_0, \ldots, T_{15}$.

<table>
<thead>
<tr>
<th>Step</th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>$T_0 \leftarrow ROTL^0(0xaaaaaaa) + X_0 + X_1 + X_2 + X_3 + X_4 + X_7$; $T_1 \leftarrow ROTL^4(X_0 + X_1 + X_3 + X_4 + X_7)$; $T_2 \leftarrow ROTL^8(X_0 + X_1 + X_4 + X_6 + X_7)$; $T_3 \leftarrow ROTL^{12}(X_2 + X_3 + X_5 + X_6 + X_7)$; $T_4 \leftarrow ROTL^{16}(X_1 + X_2 + X_3 + X_5 + X_6)$; $T_5 \leftarrow ROTL^{20}(X_0 + X_2 + X_3 + X_4 + X_6)$; $T_6 \leftarrow ROTL^{24}(X_0 + X_1 + X_5 + X_6 + X_7)$; $T_7 \leftarrow ROTL^{28}(X_2 + X_3 + X_4 + X_5 + X_6)$; $T_8 \leftarrow T_3 \oplus T_5 \oplus T_6$; $T_9 \leftarrow T_2 \oplus T_5 \oplus T_6$; $T_{10} \leftarrow T_2 \oplus T_3 \oplus T_5$; $T_{11} \leftarrow T_0 \oplus T_1 \oplus T_3$; $T_{12} \leftarrow T_0 \oplus T_4 \oplus T_7$; $T_{13} \leftarrow T_1 \oplus T_6 \oplus T_7$; $T_{14} \leftarrow T_2 \oplus T_3 \oplus T_4$; $T_{15} \leftarrow T_0 \oplus T_1 \oplus T_7$;</td>
</tr>
<tr>
<td>2.</td>
<td>$T_0 \leftarrow ROTL^0(0x55555555) + Y_0 + Y_1 + Y_2 + Y_3 + Y_5 + Y_7$; $T_1 \leftarrow ROTL^5(Y_0 + Y_1 + Y_3 + Y_4 + Y_6)$; $T_2 \leftarrow ROTL^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_5)$; $T_3 \leftarrow ROTL^{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7)$; $T_4 \leftarrow ROTL^{15}(Y_0 + Y_1 + Y_3 + Y_4 + Y_6)$; $T_5 \leftarrow ROTL^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7)$; $T_6 \leftarrow ROTL^{24}(Y_1 + Y_2 + Y_5 + Y_6 + Y_7)$; $T_7 \leftarrow ROTL^{28}(Y_0 + Y_5 + Y_4 + Y_6 + Y_7)$; $Z_5 \leftarrow T_8 + (T_3 \oplus T_4 \oplus T_6)$; $Z_6 \leftarrow T_9 + (T_2 \oplus T_5 \oplus T_7)$; $Z_7 \leftarrow T_{10} + (T_4 \oplus T_6 \oplus T_7)$; $Z_8 \leftarrow T_{11} + (T_0 \oplus T_1 \oplus T_3)$; $Z_9 \leftarrow T_{12} + (T_2 \oplus T_6 \oplus T_7)$; $Z_{10} \leftarrow T_{13} + (T_5 \oplus T_1 \oplus T_3)$; $Z_{11} \leftarrow T_{14} + (T_0 \oplus T_3 \oplus T_4)$; $Z_{12} \leftarrow T_{15} + (T_4 \oplus T_2 \oplus T_3)$;</td>
</tr>
</tbody>
</table>

$X \ast Y \equiv \pi_1(\pi_2(X) + 8 \pi_3(Y))$

$L_2 = \begin{bmatrix} 0 & 4 & 2 & 3 & 1 & 6 & 5 & 7 \\ 7 & 6 & 3 & 2 & 5 & 4 & 1 & 0 \\ 5 & 3 & 1 & 6 & 0 & 2 & 7 & 4 \\ 1 & 0 & 5 & 4 & 3 & 7 & 2 & 6 \\ 2 & 1 & 0 & 7 & 4 & 5 & 6 & 3 \\ 3 & 5 & 7 & 0 & 6 & 1 & 4 & 2 \\ 4 & 7 & 6 & 1 & 2 & 0 & 3 & 5 \\ 6 & 2 & 4 & 5 & 7 & 3 & 0 & 1 \end{bmatrix}$
Specific design characteristics for EDON-R

Quasigroup operation of order $2^{256}$

Input: $X = (X_0, X_1, \ldots, X_7)$ and $Y = (Y_0, Y_1, \ldots, Y_7)$

where $X_i$ and $Y_i$ are 32-bit variables.

Output: $Z = (Z_0, Z_1, \ldots, Z_7)$ where $Z_i$ are 32-bit variables.

Temporary 32-bit variables: $T_0, \ldots, T_{15}.$

1.

\[
\begin{align*}
T_0 & \leftarrow \text{ROTL}^9(0xAAAAAAA) + X_0 + X_1 + X_2 + X_3 + X_4 + X_7; \\
T_1 & \leftarrow \text{ROTL}^4(X_0 + X_1 + X_2 + X_3 + X_4 + X_7); \\
T_2 & \leftarrow \text{ROTL}^8(X_0 + X_1 + X_2 + X_3 + X_4 + X_7); \\
T_3 & \leftarrow \text{ROTL}^{13}(X_2 + X_3 + X_5 + X_6 + X_7); \\
T_4 & \leftarrow \text{ROTL}^{17}(X_1 + X_2 + X_3 + X_5 + X_6); \\
T_5 & \leftarrow \text{ROTL}^{22}(X_0 + X_2 + X_3 + X_4 + X_5); \\
T_6 & \leftarrow \text{ROTL}^{24}(X_0 + X_1 + X_3 + X_5 + X_6 + X_7); \\
T_7 & \leftarrow \text{ROTL}^{26}(X_2 + X_3 + X_4 + X_5 + X_6); \\
T_8 & \leftarrow T_3 \oplus T_5 \oplus T_6; \\
T_9 & \leftarrow T_2 \oplus T_5 \oplus T_7; \\
T_{10} & \leftarrow T_2 \oplus T_3 \oplus T_5; \\
T_{11} & \leftarrow T_0 \oplus T_1 \oplus T_8; \\
T_{12} & \leftarrow T_0 \oplus T_4 \oplus T_7; \\
T_{13} & \leftarrow T_1 \oplus T_6 \oplus T_7; \\
T_{14} & \leftarrow T_2 \oplus T_3 \oplus T_4; \\
T_{15} & \leftarrow T_0 \oplus T_1 \oplus T_5; \\
T_0 & \leftarrow \text{ROTL}^{9}(0x55555555) + Y_0 + Y_1 + Y_2 + Y_3 + Y_5 + Y_7; \\
T_1 & \leftarrow \text{ROTL}^{5}(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_6); \\
T_2 & \leftarrow \text{ROTL}^{9}(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_6); \\
T_3 & \leftarrow \text{ROTL}^{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7); \\
T_4 & \leftarrow \text{ROTL}^{15}(Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5); \\
T_5 & \leftarrow \text{ROTL}^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7); \\
T_6 & \leftarrow \text{ROTL}^{24}(Y_1 + Y_2 + Y_3 + Y_5 + Y_6 + Y_7); \\
T_7 & \leftarrow \text{ROTL}^{27}(Y_0 + Y_3 + Y_4 + Y_5 + Y_7); \\
Z_5 & \leftarrow T_8 \oplus (T_3 \oplus T_4 \oplus T_6); \\
Z_6 & \leftarrow T_9 \oplus (T_2 \oplus T_5 \oplus T_7); \\
Z_7 & \leftarrow T_{10} \oplus (T_4 \oplus T_6 \oplus T_7); \\
Z_8 & \leftarrow T_{11} \oplus (T_0 \oplus T_1 \oplus T_3); \\
Z_9 & \leftarrow T_{12} \oplus (T_2 \oplus T_6 \oplus T_7); \\
Z_{10} & \leftarrow T_{13} \oplus (T_0 \oplus T_4 \oplus T_7); \\
Z_{11} & \leftarrow T_{14} \oplus (T_0 \oplus T_3 \oplus T_4); \\
Z_{12} & \leftarrow T_{15} \oplus (T_1 \oplus T_2 \oplus T_5); \\
\end{align*}
\]

$X \ast Y \equiv \pi_1(\pi_2(X) + 8\pi_3(Y))$
Specific design characteristics for EDON-R

Quasigroup operation of order $2^{256}$

Input: $X = (X_0, X_1, \ldots, X_7)$ and $Y = (Y_0, Y_1, \ldots, Y_7)$

where $X_i$ and $Y_i$ are 32-bit variables.

Output: $Z = (Z_0, Z_1, \ldots, Z_7)$ where $Z_i$ are 32-bit variables.

Temporary 32-bit variables: $T_0, \ldots, T_{15}$.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_0$</td>
<td>$\text{ROT}^0_{16}(0x00000000)$</td>
<td>$X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6$</td>
</tr>
<tr>
<td>$T_1$</td>
<td>$\text{ROT}^1_{16}(0x00000000)$</td>
<td>$X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6$</td>
</tr>
<tr>
<td>$T_2$</td>
<td>$\text{ROT}^2_{16}(0x00000000)$</td>
<td>$X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6$</td>
</tr>
<tr>
<td>$T_3$</td>
<td>$\text{ROT}^3_{16}(0x00000000)$</td>
<td>$X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6$</td>
</tr>
<tr>
<td>$T_4$</td>
<td>$\text{ROT}^4_{16}(0x00000000)$</td>
<td>$X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6$</td>
</tr>
<tr>
<td>$T_5$</td>
<td>$\text{ROT}^5_{16}(0x00000000)$</td>
<td>$X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6$</td>
</tr>
<tr>
<td>$T_6$</td>
<td>$\text{ROT}^6_{16}(0x00000000)$</td>
<td>$X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6$</td>
</tr>
<tr>
<td>$T_7$</td>
<td>$\text{ROT}^7_{16}(0x00000000)$</td>
<td>$X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6$</td>
</tr>
</tbody>
</table>

1. $T_0 \leftarrow T_0 \oplus T_1 \oplus T_2 \oplus T_3 \oplus T_4 \oplus T_5 \oplus T_6 \oplus T_7$

2. $T_0 \leftarrow \text{ROT}^0_{16}(0x00000000)$

3. $T_0 \leftarrow \text{ROT}^0_{16}(0x00000000)$

4. $Z_0 \leftarrow Z_0 \oplus T_3 \oplus T_4 \oplus T_5 \oplus T_6 \oplus T_7$

Rotations differ from each other for at least 2 positions.

$$X \ast Y \equiv \pi_1(\pi_2(X) + 8 \pi_3(Y))$$
Specific design characteristics for EDON-R

\[ L_1 = \begin{bmatrix} 0 & 7 & 1 & 3 & 2 & 4 & 6 & 5 \\ 4 & 1 & 7 & 6 & 3 & 0 & 5 & 2 \\ 7 & 0 & 4 & 2 & 5 & 3 & 1 & 6 \\ 1 & 4 & 0 & 5 & 6 & 2 & 7 & 3 \\ 2 & 3 & 6 & 7 & 1 & 5 & 0 & 4 \\ 5 & 2 & 3 & 1 & 7 & 6 & 4 & 0 \\ 3 & 6 & 5 & 0 & 4 & 7 & 2 & 1 \\ 6 & 5 & 2 & 4 & 0 & 1 & 3 & 7 \end{bmatrix} = \begin{bmatrix} L_{1,1} \\ L_{1,2} \end{bmatrix} \]

\[ L_2 = \begin{bmatrix} 0 & 4 & 2 & 3 & 1 & 6 & 5 & 7 \\ 7 & 6 & 3 & 2 & 5 & 4 & 1 & 0 \\ 5 & 3 & 1 & 6 & 0 & 2 & 7 & 4 \\ 1 & 0 & 5 & 4 & 3 & 7 & 2 & 6 \\ 2 & 1 & 0 & 7 & 4 & 5 & 6 & 3 \\ 3 & 5 & 7 & 0 & 6 & 1 & 4 & 2 \\ 4 & 7 & 6 & 1 & 2 & 0 & 3 & 5 \\ 6 & 2 & 4 & 5 & 7 & 3 & 0 & 1 \end{bmatrix} = \begin{bmatrix} L_{2,1} \\ L_{2,2} \end{bmatrix} \]

Two orthogonal Latin Squares of order 8
Specific design characteristics for EDON-R

Two orthogonal Latin Squares of order 8

Four corresponding nonsingular in \((\mathbb{Z}_2, +, \times)\) matrices.
Specific design characteristics for EDON-R

Four nonsingular in \((\mathbb{Z}_2, +, \cdot)\) matrices.

\[
\begin{align*}
A_1 &= \begin{pmatrix}
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}, &
A_2 &= \begin{pmatrix}
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1
\end{pmatrix}, &
A_3 &= \begin{pmatrix}
1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 1
\end{pmatrix}, &
A_4 &= \begin{pmatrix}
0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0
\end{pmatrix}
\end{align*}
\]
Specific design characteristics for EDON-R

Four nonsingular in \((\mathbb{Z}_2, +, \times)\) matrices.

\[
A_1 = \begin{pmatrix}
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0
\end{pmatrix} \quad A_2 = \begin{pmatrix}
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix} \quad A_3 = \begin{pmatrix}
1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 1
\end{pmatrix} \quad A_4 = \begin{pmatrix}
0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0
\end{pmatrix}
\]

Two diffusion (bi-stochastic) matrices

\[
\text{Diff}_{\pi_2} = (A_1 \cdot A_2)^T \quad \text{Diff}_{\pi_3} = (A_3 \cdot A_4)^T
\]

\[
\begin{pmatrix}
2 & 3 & 2 & 2 & 1 & 2 & 1 & 2 \\
1 & 2 & 1 & 3 & 2 & 2 & 2 & 2 \\
2 & 1 & 2 & 2 & 3 & 1 & 2 & 2 \\
2 & 1 & 2 & 2 & 2 & 2 & 2 & 2 \\
1 & 2 & 2 & 2 & 2 & 2 & 1 & 3 \\
3 & 2 & 2 & 1 & 2 & 2 & 2 & 1 \\
2 & 2 & 2 & 1 & 2 & 2 & 3 & 1 \\
2 & 2 & 2 & 1 & 2 & 2 & 2 & 2
\end{pmatrix} \quad \begin{pmatrix}
1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
2 & 1 & 2 & 2 & 2 & 2 & 2 & 2 \\
2 & 2 & 1 & 2 & 2 & 2 & 2 & 2 \\
2 & 2 & 1 & 2 & 2 & 2 & 2 & 2 \\
2 & 2 & 2 & 2 & 1 & 2 & 2 & 2 \\
2 & 2 & 2 & 1 & 2 & 2 & 1 & 2 \\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 1
\end{pmatrix}
\]
### Specific design characteristics for EDON-R

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. $L_1$ and $L_2$ are orthogonal Latin squares.</td>
<td>8 $w$-bit variables belonging to $X$ are to be mixed with 8 $w$-bit variables belonging to $Y$ in such a way that all pairs are combined by some operation (addition, or XORing).</td>
</tr>
<tr>
<td>2. $\text{Diff}<em>{\pi_2}$ and $\text{Diff}</em>{\pi_3}$ do not have zeroes.</td>
<td>The situation where $X \ast_q Y = Z$ and some difference either in $X$ or in $Y$ will not affect some of the eight words of $Z$ are to be avoided.</td>
</tr>
<tr>
<td>3. Elements of the matrix $\text{Diff}_{\pi_2}$ have the biggest possible variance.</td>
<td>This is an analogy to the &quot;confusion&quot; principle in cryptology. Choosing $\text{Diff}_{\pi_2}$ with the biggest possible variance improves the resistance against cryptanalysis because there is no regular pattern how the computations are performed.</td>
</tr>
<tr>
<td>4. Elements of the matrix $\text{Diff}_{\pi_3}$ have the smallest possible variance.</td>
<td>This is an analogy to the &quot;diffusion&quot; principle in cryptology. Choosing $\text{Diff}_{\pi_3}$ with the smallest possible variance increases the diffusion of the bit differences in the greatest possible way, with the smallest possible variances in the pattern of the computations that are performed.</td>
</tr>
</tbody>
</table>

**Table 3.9:** Criteria for choosing the Latin squares
Specific design characteristics for EDON-R

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. $L_1$ and $L_2$ are orthogonal Latin squares.</td>
<td>$8 \ w$-bit variables belonging to $X$ are to be mixed with $8 \ w$-bit variables belonging to $Y$ in such a way that all pairs are combined by some operation (addition, or XORing). The situation where $X \cdot_q Y = Z$ and some difference either</td>
</tr>
<tr>
<td></td>
<td>has the smallest possible variance.</td>
</tr>
<tr>
<td></td>
<td>cryptology. Choosing $\text{Diff}_{\pi_3}$ with the smallest possible variance increases the diffusion of the bit differences in the greatest possible way, with the smallest possible variances in the pattern of the computations that are performed.</td>
</tr>
</tbody>
</table>

Table 3.9: Criteria for choosing the Latin squares
Specific design characteristics for EDON-R

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. $L_1$ and $L_2$ are orthogonal Latin squares.</td>
<td>$8w$-bit variables belonging to $X$ are to be mixed with $8w$-bit variables belonging to $Y$ in such a way that all pairs are combined by some operation (addition, or XORing).</td>
</tr>
<tr>
<td>2. $\text{Diff}<em>{\pi_2}$ and $\text{Diff}</em>{\pi_3}$ do not have zeroes.</td>
<td>The situation where $X \cdot_q Y = Z$ and some difference either in $X$ or in $Y$ will not affect some of the eight words of $Z$ are to be avoided.</td>
</tr>
<tr>
<td>3. Elements of $L_2$ have the biggest 8-bit differences in the pattern of the computations that are performed.</td>
<td>“Principle in the biggest possible way the computations against cryptanalysis” principle in “smallest possible bit differences in the worst possible variances&quot; principle in.</td>
</tr>
<tr>
<td>4. Elements of $L_2$ have the smallest possible variances</td>
<td>“Principle in the biggest possible way the computations against cryptanalysis” principle in “smallest possible bit differences in the worst possible variances&quot; principle in.</td>
</tr>
</tbody>
</table>

Table 3.9: Criteria for choosing the Latin squares
<table>
<thead>
<tr>
<th>Edon-R Latin</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>$23221212$</td>
<td>$8$ $w$-bit variables belonging to $X$ are to be mixed with $8$ $w$-bit variables belonging to $Y$ in such a way that all pairs are combined by some operation (addition, or XORing).</td>
</tr>
<tr>
<td>$12132222$</td>
<td>The situation where $X \ast_q Y = Z$ and some difference either in $X$ or in $Y$ will not affect some of the eight words of $Z$ are to be avoided.</td>
</tr>
</tbody>
</table>

3. Elements of the matrix $\text{Diff}_{\pi_2}$ have the biggest possible variance. This is an analogy to the "confusion" principle in cryptology. Choosing $\text{Diff}_{\pi_2}$ with the biggest possible variance improves the resistance against cryptanalysis because there is no regular pattern how the computations are performed.

4. Elements of the matrix $\text{Diff}_{\pi_3}$ have the smallest possible variance. This is an analogy to the "diffusion" principle in cryptology. Choosing $\text{Diff}_{\pi_3}$ with the smallest possible variance increases the diffusion of the bit differences in the greatest possible way, with the smallest possible variances in the pattern of the computations that are performed.

**Table 3.9:** Criteria for choosing the Latin squares
### Specific design characteristics for Cryptographic Hash Function EDON-R

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (L_1) and (L_2) are orthogonal Latin squares.</td>
<td>(8w)-bit variables belonging to (X) and (w)-bit variables belonging to (Y) in (X) are combined by some operation. The situation where (X \cdot q \cdot Y = Z) are in (X) or in (Y) will not affect some of the (z) to be avoided.</td>
</tr>
<tr>
<td>2. (\text{Diff}<em>{\pi_2}) and (\text{Diff}</em>{\pi_3}) do not have zeroes.</td>
<td>This is an analogy to the &quot;confusion&quot; principle in cryptology. Choosing (\text{Diff}_{\pi_2}) with the biggest possible variance improves the resistance against cryptanalysis because there is no regular pattern how the computations are performed.</td>
</tr>
<tr>
<td>3. Elements of the matrix (\text{Diff}_{\pi_2}) have the biggest possible variance.</td>
<td>This is an analogy to the &quot;diffusion&quot; principle in cryptology. Choosing (\text{Diff}_{\pi_3}) with the smallest possible variance increases the diffusion of the bit differences in the greatest possible way, with the smallest possible variances in the pattern of the computations that are performed.</td>
</tr>
<tr>
<td>4. Elements of the matrix (\text{Diff}_{\pi_3}) have the smallest possible variance.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 3.9:** Criteria for choosing the Latin squares
Specific design characteristics for EDON-R

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. $L_1$ and $L_2$ are orthogonal Latin squares.</td>
<td>$8w$-bit variables belonging to $X$ are to be mixed with $8w$-bit variables belonging to $Y$ in such a way that all pairs are combined by some operation (addition, or XORing). The situation where $X \ast_q Y = Z$ and some difference either</td>
</tr>
<tr>
<td></td>
<td>$\neq 0$ in the field $\mathbb{F}_2^q$.</td>
</tr>
<tr>
<td>2. Diff$<em>{\pi_1}$ and Diff$</em>{\pi_2}$ do not have common columns.</td>
<td>We took all $2^{165}$ main classes of orthogonal Latin Sqaures of order $8$ from Brendan McKay’s web page <a href="http://cs.anu.edu.au/people/bdm/data/latin.html">http://cs.anu.edu.au/people/bdm/data/latin.html</a> and searched trough $(8!)^2 \approx 2^{30.6}$ pairs of orthogonal isotopes. We found that</td>
</tr>
<tr>
<td></td>
<td>Latin Squares that comply maximal variance $19/63$ and minimal variance $1/9$. We took the first such pair for EDON-R.</td>
</tr>
<tr>
<td>3. Elements of the matrix Diff$_{\pi_3}$ have the smallest possible variance.</td>
<td>This is an analogy to the &quot;diffusion&quot; principle in cryptology. Choosing Diff$_{\pi_3}$ with the smallest possible variance increases the diffusion of the bit differences in the greatest possible way, with the smallest possible variances in the pattern of the computations that are performed.</td>
</tr>
<tr>
<td>4. Elements of the matrix Diff$_{\pi_3}$ have the smallest possible variance.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 3.9:** Criteria for choosing the Latin squares
Specific design characteristics for EDON-R

Definition 12. Let \( X, X', Y, Y' \in Q_q \) and let \( \Delta_X = X \oplus X' \) and \( \Delta_Y = Y \oplus Y' \) be two difference vectors. Let \( Z = X \ast_q Y \) and \( Z' = X' \ast_q Y' \). The vector \( D_{(\Delta_X, \Delta_Y)} = (\delta_0, \ldots, \delta_7) \in (Z)^8 \) is called bit flip counter for the quasigroup operation \( \ast_q \), if every \( \delta_i, i = 0, \ldots, 7 \) is a counter of the minimal number of bit flips that the quasigroup operation \( \ast_q \) performs to transfer the value \( Z \) to the value \( Z' \).

Theorem 3: \[ D_{(\Delta_X, \Delta_Y)} = \text{Diff}_{\pi_2} \cdot \Delta_X + \text{Diff}_{\pi_3} \cdot \Delta_Y \]
Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis

<table>
<thead>
<tr>
<th></th>
<th>$\Delta_\chi$</th>
<th>$\Delta_Y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\bar{\Delta}_Y$</td>
<td>$D_1 = \text{Diff}<em>{\pi_2} \cdot \bar{\Delta}<em>Y + \text{Diff}</em>{\pi_3} \cdot \Delta</em>\chi$</td>
<td>$D_2 = \text{Diff}<em>{\pi_2} \cdot D_1 + \text{Diff}</em>{\pi_3} \cdot \Delta_Y$</td>
</tr>
<tr>
<td>0</td>
<td>$D_3 = \text{Diff}<em>{\pi_2} \cdot 0 + \text{Diff}</em>{\pi_3} \cdot D_1$</td>
<td>$D_4 = \text{Diff}<em>{\pi_2} \cdot D_3 + \text{Diff}</em>{\pi_3} \cdot D_2$</td>
</tr>
<tr>
<td>0</td>
<td>$D_5 = \text{Diff}<em>{\pi_2} \cdot D_3 + \text{Diff}</em>{\pi_3} \cdot 0$</td>
<td>$D_6 = \text{Diff}<em>{\pi_2} \cdot D_4 + \text{Diff}</em>{\pi_3} \cdot D_5$</td>
</tr>
<tr>
<td>$\bar{\Delta}_\chi$</td>
<td>$D_7 = \text{Diff}<em>{\pi_2} \cdot \bar{\Delta}</em>\chi + \text{Diff}_{\pi_3} \cdot D_5$</td>
<td>$D_8 = \text{Diff}<em>{\pi_2} \cdot D_7 + \text{Diff}</em>{\pi_3} \cdot D_6$</td>
</tr>
</tbody>
</table>
### Specific design characteristics for EDON-R

**EDON-R is provably resistant against differential cryptanalysis**

<table>
<thead>
<tr>
<th>$\overline{\Delta_x} = (0,0,0,0,0,0,0,0)$</th>
<th>$\overline{\Delta_y} = (0,0,0,0,0,0,0,0)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta_y = (0,0,0,0,0,0,0,0)$</td>
<td>$(1,2,2,2,2,2,2,2)$</td>
</tr>
<tr>
<td>$0$</td>
<td>$(29,28,28,28,28,28,28,28)$</td>
</tr>
<tr>
<td>$0$</td>
<td>$(422,421,422,422,421,423,422,422)$</td>
</tr>
<tr>
<td>$\overline{\Delta_x} = (0,0,0,0,0,0,0,1)$</td>
<td>$(6330,6331,6330,6330,6332,6328,6329,6330)$</td>
</tr>
<tr>
<td></td>
<td>$(379716,379715,379721,379713,379716,379717,379715,379712)$</td>
</tr>
</tbody>
</table>

**Table 3.6:** Vectors of minimal number of bit flips for the function $R$ when the initial difference vectors are $\Delta_x = (1,0,0,0,0,0,0,0)$ and $\Delta_y = (0,0,0,0,0,0,0,0)$.

<table>
<thead>
<tr>
<th>$\overline{\Delta_x} = (0,0,0,0,0,0,0,0)$</th>
<th>$\overline{\Delta_y} = (1,0,0,0,0,0,0,0)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta_y = (0,0,0,0,0,0,0,0)$</td>
<td>$(2,2,2,2,3,1,1,2)$</td>
</tr>
<tr>
<td>$0$</td>
<td>$(28,28,28,28,27,29,29,28)$</td>
</tr>
<tr>
<td>$0$</td>
<td>$(422,422,420,422,421,422,423,423)$</td>
</tr>
<tr>
<td>$\overline{\Delta_x} = (0,0,0,0,0,0,0,0)$</td>
<td>$(6328,6328,6330,6328,6329,6328,6327,6327)$</td>
</tr>
<tr>
<td></td>
<td>$(386016,386011,386017,386016,386016,386018,386017,386014)$</td>
</tr>
</tbody>
</table>

**Table 3.7:** Vectors of minimal number of bit flips for the function $R$ when the initial difference vectors are $\Delta_x = (0,0,0,0,0,0,0,0)$ and $\Delta_y = (1,0,0,0,0,0,0,0)$. 
Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis

| $\Delta_y = (0,0,0,0,0,0,0)$ | $\Delta_x = (1,0,0,0,0,0,0)$ | $\Delta_y = (0,0,0,0,0,0,0)$ |
| $\Delta_x = (0,0,0,0,0,0,0,1)$ | $\Delta_x = (0,0,0,0,0,0,0,0)$ | $\Delta_y = (1,0,0,0,0,0,0,0)$ |

$\Delta_x = (0,0,0,0,0,0,0,0)$

$\Delta_y = (0,0,0,0,0,0,0,0)$

$\Delta_y = (0,0,0,0,0,0,0,0,1)$

$\Delta_y = (0,0,0,0,0,0,0,0,0)$

$\Delta_y = (0,0,0,0,0,0,0,0,0)$

Note the variance of the elements!

Table 3.7: Vectors of minimal number of bit flips for the function $\mathcal{R}$ when the initial difference vectors are $\Delta_x = (0,0,0,0,0,0,0,0)$ and $\Delta_y = (1,0,0,0,0,0,0,0)$.  

Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis

<table>
<thead>
<tr>
<th>$\Delta X = (1, 0, 0, 0, 0, 0, 0, 0)$</th>
<th>$\Delta Y = (0, 0, 0, 0, 0, 0, 0, 0)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta Y = (0, 0, 0, 0, 0, 0, 0, 0)$</td>
<td>$(1, 2, 2, 2, 2, 2, 2, 2)$</td>
</tr>
<tr>
<td>0</td>
<td>$(29, 28, 28, 28, 28, 28, 28, 28)$</td>
</tr>
<tr>
<td>0</td>
<td>$(422, 421, 422, 422, 421, 423, 422)$</td>
</tr>
<tr>
<td>$\Delta X = (0, 0, 0, 0, 0, 0, 0, 1)$</td>
<td>$(6330, 6331, 6330, 6330, 6332, 6328, 6329, 6330)$</td>
</tr>
</tbody>
</table>

Table 3.7: Vectors of minimal number of bit flips for the function $R$ when the initial difference vectors are $\Delta X = (0, 0, 0, 0, 0, 0, 0, 0)$ and $\Delta Y = (1, 0, 0, 0, 0, 0, 0, 0)$.

Theorem 4. The variance of the elements of the $D_i$, $i = 1, \ldots, 8$ decreases (relative to the minimal element in the vectors $D_i$, $i = 1, \ldots, 8$), with every row of quasigroup string transformations in the compression function $R$. □
Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis

Theorem 5. Let $D_i = (\delta_0^{(i)}, \delta_1^{(i)}, \ldots, \delta_7^{(i)})$, $i = 1, \ldots, 8$ be a vector of minimal number of bit flips for the function $R$ where the size of the word is $w$ bits ($w = 32, 64$), and let $\Delta_{D_i} = (\Delta_0^{(i)}, \Delta_1^{(i)}, \ldots, \Delta_7^{(i)}) = \left(\Delta_0^{(i)}, \ldots, \Delta_{w-1}^{(i)}, \Delta_w^{(i)}, \ldots, \Delta_{2w-1}^{(i)}, \Delta_{2w}^{(i)}, \ldots, \Delta_{7w-1}^{(i)}, \Delta_{7w}^{(i)}, \ldots, \Delta_{8w-1}^{(i)}\right)$, $i = 1, \ldots, 8$ (where $\Delta_j^{(i)} \in \{0, 1\}$, $j = 0, \ldots, 8w - 1$) are the corresponding differentials in the intermediate variables $\Delta_{D_i}$ for some initially chosen differentials $\Delta_X$ and $\Delta_Y$ (where at least one of them is a non-zero differential). If the number of bit flips for every single bit is equally distributed then the probabilities that every difference bit $\Delta_j^{(i)}$ is 0 or 1 are given as:

$$Pr(\Delta_j^{(i)} = 0 | \Delta_X, \Delta_Y) = 0.5 + \epsilon_{\delta_j^{(i)}},$$

$$Pr(\Delta_j^{(i)} = 1 | \Delta_X, \Delta_Y) = 0.5 - \epsilon_{\delta_j^{(i)}},$$

where $\mu = \left\lfloor \frac{i}{w} \right\rfloor$ and $\epsilon_{\delta_j^{(i)}} \leq 0.5 \left(\frac{w-2}{w}\right)^{\delta_j^{(i)}}$. 

Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis

Theorem 5. Let $D_i = (\delta_0^{(i)}, \delta_1^{(i)}, \ldots, \delta_7^{(i)})$, $i = 1, \ldots, 8$ be a vector of minimal number of bit flips for the function $R$ where the size of the word is $w$ bits ($w = 32, 64$), and let $\Delta D_i = (\Delta_0^{(i)}, \Delta_1^{(i)}, \ldots, \Delta_7^{(i)}) = (\Delta_0^{(i)}, \ldots, \Delta_{w-1}^{(i)}, \Delta_1^{(i)}, \ldots, \Delta_{2w-1}^{(i)}, \Delta_2^{(i)}, \ldots, \Delta_{7w-1}^{(i)}, \Delta_3^{(i)}, \ldots, \Delta_{8w-1}^{(i)}$, $i = 1, \ldots, 8$ (where $\Delta_j^{(i)} \in \{0, 1\}$, $j = 0, \ldots, 8w - 1$) are the corresponding differentials in the intermediate variables $\Delta D_i$ for some initially chosen differentials $\Delta X$ and $\Delta Y$ (where at least one of them is a non-zero differential). If the number of bit flips for every single bit is equally distributed then the probabilities that every difference bit $\Delta_j^{(i)}$ is 0 or 1 are given as:

$$Pr(\Delta_j^{(i)} = 0|\Delta X, \Delta Y) = 0.5 + \epsilon_{\delta_j^{(i)}},$$

$$Pr(\Delta_j^{(i)} = 1|\Delta X, \Delta Y) = 0.5 - \epsilon_{\delta_j^{(i)}},$$

where $\mu = \left\lfloor \frac{i}{w} \right\rfloor$ and $\epsilon_{\delta_j^{(i)}} \leq 0.5 \left( \frac{w-2}{w} \right)^{\delta_j^{(i)}}$. 
Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis

Theorem 5. Let \( D_i = (\delta_0^{(i)}, \delta_1^{(i)}, \ldots, \delta_7^{(i)}) \), \( i = 1, \ldots, 8 \) be a vector of minimal number of bit flips for the function \( R \) where the size of the word is \( w \) bits \((w = 32, 64)\), and let \( \Delta_{D_i} = (\Delta_0^{(i)}, \Delta_1^{(i)}, \ldots, \Delta_7^{(i)}) = (\Delta_{w-1}^{(i)}, \Delta_{2w-1}^{(i)}, \ldots, \Delta_{7w-1}^{(i)}, \Delta_{7w}^{(i)}, \ldots, \Delta_{8w-1}^{(i)}) \), \( i = 1, \ldots, 8 \) (where \( \Delta_j^{(i)} \in \{0, 1\} \), \( j = 0, \ldots, 8w - 1 \)) are the corresponding differentials in the intermediate variables \( \Delta_{D_i} \) for some initially chosen differentials \( \Delta_X \) and \( \Delta_Y \) (where at least one of them is a non-zero differential). If the number of bit flips for every single bit is equally distributed then the probabilities that every difference bit \( \Delta_j^{(i)} \) is 0 or 1 are given as:

\[
    Pr(\Delta_j^{(i)} = 0|\Delta_X, \Delta_Y) = 0.5 + \varepsilon_{\Delta_j^{(i)}}, \\
    Pr(\Delta_j^{(i)} = 1|\Delta_X, \Delta_Y) = 0.5 - \varepsilon_{\Delta_j^{(i)}},
\]

where \( \mu = \left\lfloor \frac{i}{w} \right\rfloor \) and \( \varepsilon_{\Delta_j^{(i)}} \leq 0.5 \left( \frac{w-2}{w} \right) \delta_{\Delta_j^{(i)}} \).
Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis

Theorem 5. Let $D_i = (\delta_0^{(i)}, \delta_1^{(i)}, \ldots, \delta_7^{(i)})$, $i = 1, \ldots, 8$ be a vector of minimal number of bit flips for the function $R$ where the size of the word is $w$ bits ($w = 32, 64$), and let $\Delta_{D_i} = (\Delta_{D_0}^{(i)}, \Delta_{D_1}^{(i)}, \ldots, \Delta_{D_7}^{(i)}) = (\Delta_0^{(i)}, \ldots, \Delta_{w-1}^{(i)}, \Delta_w^{(i)}, \ldots, \Delta_{2w-1}^{(i)}, \Delta_{2w}^{(i)}, \ldots, \Delta_{7w-1}^{(i)}, \Delta_{7w}^{(i)}, \ldots, \Delta_{8w-1}^{(i)})$, $i = 1, \ldots, 8$ (where $\Delta_j^{(i)} \in \{0, 1\}$, $j = 0, \ldots, 8w - 1$) are the corresponding differentials in the intermediate variables $\Delta_{D_j}$ for some initially chosen differentials $\Delta_X$ and $\Delta_Y$ (where at least one of them is a non-zero differential). If the number of bit flips for every single bit is equally distributed then the probabilities that every difference bit $\Delta_j^{(i)}$ is 0 or 1 are given as:

$$Pr(\Delta_j^{(i)} = 0 | \Delta_X, \Delta_Y) = 0.5 + \varepsilon_{\delta_j^{(i)}},$$

$$Pr(\Delta_j^{(i)} = 1 | \Delta_X, \Delta_Y) = 0.5 - \varepsilon_{\delta_j^{(i)}},$$

where $\mu = \left\lfloor \frac{i}{w} \right\rfloor$ and $\varepsilon_{\delta_j^{(i)}} \leq 0.5 \left( \frac{w - 2}{w} \right) \delta_{\mu}^{(i)}$. 
Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis

Theorem 5. Let $D_i = (\delta_0^{(i)}, \delta_1^{(i)}, \ldots, \delta_7^{(i)})$, $i = 1, \ldots, 8$ be a vector of minimal number of bit flips for the function $\mathcal{R}$ where the size of the word is $w$ bits ($w = 32, 64$), and let $\Delta D_i = (\Delta_0^{(i)}, \Delta_1^{(i)}, \ldots, \Delta_7^{(i)}) = (\Delta_0^{(i)}, \ldots, \Delta_{w-1}^{(i)}, \Delta_w^{(i)}, \ldots, \Delta_{2w-1}^{(i)}, \Delta_{2w}^{(i)}, \ldots, \Delta_{7w-1}^{(i)}, \Delta_{7w}^{(i)}, \ldots, \Delta_{8w-1}^{(i)})$, $i = 1, \ldots, 8$ (where $\Delta_j^{(i)} \in \{0, 1\}$, $j = 0, \ldots, 8w - 1$) are the corresponding differentials in the intermediate variables $\Delta D_i$ for some initially chosen differentials $\Delta X$ and $\Delta Y$ (where at least one of them is a non-zero differential). If the number of bit flips for every single bit is equally distributed then the probabilities that every difference bit $\Delta_j^{(i)}$ is 0 or 1 are given as:

$$Pr(\Delta_j^{(i)} = 0 | \Delta X, \Delta Y) = 0.5 + \epsilon_{\delta_\mu}^{(i)},$$

$$Pr(\Delta_j^{(i)} = 1 | \Delta X, \Delta Y) = 0.5 - \epsilon_{\delta_\mu}^{(i)},$$

where $\mu = \left\lfloor \frac{i}{w} \right\rfloor$ and $\epsilon_{\delta_\mu}^{(i)} \leq 0.5 \left( \frac{w-2}{w} \right) \delta^{(i)}_{\mu}$.
Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis

<table>
<thead>
<tr>
<th>$\Delta_X = (1, 0, 0, 0, 0, 0, 0, 0)$</th>
<th>$\Delta_Y = (0, 0, 0, 0, 0, 0, 0, 0)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$w = 32$</td>
<td>$w = 64$</td>
</tr>
<tr>
<td>$\epsilon \leq 2^{-1.09}$</td>
<td>$\epsilon \leq 2^{-1.05}$</td>
</tr>
<tr>
<td>$\epsilon \leq 2^{-3.61}$</td>
<td>$\epsilon \leq 2^{-2.28}$</td>
</tr>
<tr>
<td>$\epsilon \leq 2^{-40.20}$</td>
<td>$\epsilon \leq 2^{-20.28}$</td>
</tr>
<tr>
<td>$\epsilon \leq 2^{-590.20}$</td>
<td>$\epsilon \leq 2^{-290.85}$</td>
</tr>
</tbody>
</table>

Table 3.8: Upper bounds for the deviations $\epsilon$. The probability that a bit will have a differential $\Delta = 1$ is $0.5 - \epsilon$, and the probability that a bit will have a differential $\Delta = 0$ is $0.5 + \epsilon$. The initial difference vectors are $\Delta_X = (1, 0, 0, 0, 0, 0, 0, 0)$ and $\Delta_Y = (0, 0, 0, 0, 0, 0, 0, 0)$. 
Specific design characteristics for EDON-R

EDON-R has double size chaining (pipe) values

- For n=224, 256, chaining value has 512 bits
- For n=384, 512, chaining value has 1024 bits

- Gives resistance against length-extension attack
- Gives resistance against multi-collision attack
Known attacks on EDON-R

1. Khovratovic and Nikolic
   • Free-start collisions in Edon-R
   • Using free-start collisions to launch preimage attack with \( \text{TIME} \sim O(2^{2n/3}) \) and \( \text{MEMORY} \sim O(2^{2n/3}) \) i.e. the attack has this property:
     \[
     \text{TIME} \times \text{MEMORY} > 2^n + n/3 \gg 2^n
     \]

2. Klima: EDON-R is "almost" as ordinary strengthened MD design.
   • That "almost" is in the small additional factor of \( 2^{65} \) to the generic multicollision attack that comes from the Merkle-Damgård strengthening.
Known attacks on EDON-R

1. Khovratovic and Nikolic
   • Free-start collisions in Edon-R
     • Using free-start collisions to launch preimage attack with \( \text{TIME} \sim O(2^{2n/3}) \) and \( \text{MEMORY} \sim O(2^{2n/3}) \) i.e. the attack has this property:
       \[
       \text{TIME} \times \text{MEMORY} > 2^n + \frac{n}{3} \gg 2^n
       \]

2. Klima: **EDON-R is "almost"** as ordinary strengthened MD design.
   • That "almost" is in the small additional factor of \( 2^{65} \) to the generic multicollision attack that comes from the Merkle-Damgård strengthening.

Idea to defend from both attacks **without changing anything in the definition of the compression function**

**Make the Merkle-Damgård strengthening of EDON-R to be 129 bits (instead of the current 65 bit strengthening).**
Are there one-way bijections embedded in EDON-R?

Example:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Are there one-way bijections embedded in EDON-R?

Example:

1. Fix $C_0 = 1$, $C_1 = 0$, $B_0 = 2$, $B_1 = 3$.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Are there one-way bijections embedded in EDON-R?

Example:

<table>
<thead>
<tr>
<th>*</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

1. Fix $C_0 = 1$, $C_1 = 0$, $B_0 = 2$,
2. For every $A_0$ in $\{0, 1, 2, 3\}$, compute:
   1. $X_0^{(3)}$,
   2. $X_0^{(2)}$,
   3. $X_0^{(1)}$,
   4. $A_1$,
   5. $X_1^{(1)}$,
   6. $X_1^{(2)}$,
   7. $X_1^{(3)}$,
   8. $B_1$,
Are there one-way bijections embedded in EDON-R?

Example:

1. Fix $C_0=1$, $C_1=0$, $B_0=2$.
2. For every $A_0$ in $\{0,1,2,3\}$, compute:
   1. $X_0^{(3)}$,
   2. $X_0^{(2)}$,
   3. $X_0^{(1)}$,
   4. $A_1$,

<table>
<thead>
<tr>
<th>*</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

1. The mapping: $A_0 \rightarrow B_1$ is a bijection.
2. Knowing $A_0$, it is easy to compute $B_1$.
3. However: Knowing $B_1$, it is “hard” to find $A_0$.
4. For tiny quasigroups of order 4 we found that 144 quasigroups give bijections for every value of $C_0$, $C_1$ and $B_0$. 
Are there one-way bijections embedded in EDON-R?

Example:

<table>
<thead>
<tr>
<th>*</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

1. Fix $C_0=1$, $C_1=0$, $B_0=2$,
2. For every $A_0$ in \{0,1,2,3\}, compute:
   1. $X_0^{(3)}$,
   2. $X_0^{(2)}$,
   3. $X_0^{(1)}$,
   4. $A_1$,
   5. $X_1^{(1)}$,
   6. $X_1^{(2)}$,
   7. $X_1^{(3)}$,
   8. $B_1$,

Hypothesis: For certain values of $C_0$, $C_1$, $B_0$, one-way bijections can be defined by EDON-R compression function.
## SW/HW performance and memory requirements

<table>
<thead>
<tr>
<th>Software performances of the optimized C implementation on the NIST reference platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel C++ v11.0.66, in 64-bit mode</td>
</tr>
<tr>
<td>EDON-R 224/256 achieves <strong>4.54 cycles/byte</strong></td>
</tr>
<tr>
<td>Intel C++ v11.0.66, in 64-bit mode</td>
</tr>
<tr>
<td>EDON-R 384/512 achieves <strong>2.29 cycles/byte</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Memory requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDON-R 224/256 needs <strong>256 bytes</strong></td>
</tr>
<tr>
<td>EDON-R 384/512 needs <strong>512 bytes</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HW – gate count</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDON-R 224/256, ~13,000 gates</td>
</tr>
<tr>
<td>EDON-R 384/512, ~25,000 gates</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8-bit MCU (ATmega16, ATmega406)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDON-R 224/256, compiled C code produces ~6KB of machine instructions, speed 616 cycles/bytes</td>
</tr>
<tr>
<td>EDON-R 384/512, compiled C code produces ~38KB of machine instructions, speed 1857 cycles/bytes</td>
</tr>
</tbody>
</table>
Thank you for your attention!