IMPORTANT FEATURES AND FLEXIBILITIES OF TRIVIA

Avik Chakraborti, Mridul Nandi

Indian Statistical Institute, Kolkata

August 24, 2014
DIAC, UCSB
OUTLINE

1. **TriviA AE Scheme**
2. **Features of TriviA**
3. **Possible Proposed Modification of TriviA**
1. **TriviA AE Scheme**
   - SC-TriviA: Underlying Streamcipher
   - VPV Hash
   - Security

2. **Features of TriviA**

3. **Possible Proposed Modification of TriviA**
Avik Chakraborti, Mridul Nandi

**Important Features and Flexibilities of TriviA**

- **SC-TriviA** - Updated version of Trivium.
- **VPV-Hash** - Universal Hash follows EHC technique.
- SC-TriviA generates encryption and authentication key stream.
**Key Information of TriviA**

- **SC-TriviA** uses 128-bit key and 128-bit nonce.
- **Block Size** $w$ - 64-bit
- **Underlying Field** - $F_{2^{32}}$ and $F_{2^{64}}$
- Encrypts message by *One-Time-Pad*.
- Intermediate tag - Computed after each $ck$ blocks.
- Size of each of the tags - 128-bit
**Recommended Parameter Choice**

- $ck$ varies from 0 to $2^{30}$
- $ck = 0 \implies$ No intermediate tag.

**We Recommend Two Versions**

- TriviA-0 with $ck = 0$ and
- TriviA-128 with $ck = 128$
NFSR (nonlinear feedback): $|A| = 132, |B| = 105, |C| = 147$. 
Key Extraction and State Updation for SC-TriviA

Key Extraction and State Updation for 64 rounds

1. \( t_1 \leftarrow A_{[3\ldots66]} \oplus A_{[69\ldots132]} \oplus A_{[67\ldots130]} \land A_{[68\ldots131]} \oplus B_{[33\ldots96]} \)
2. \( t_2 \leftarrow B_{[6\ldots69]} \oplus B_{[42\ldots105]} \oplus B_{[40\ldots103]} \land B_{[41\ldots104]} \oplus C_{[57\ldots120]} \)
3. \( t_3 \leftarrow C_{[3\ldots66]} \oplus C_{[84\ldots147]} \oplus C_{[82\ldots145]} \land C_{[83\ldots146]} \oplus A_{[12\ldots75]} \)
4. \((A_1, A_2, A_3, \ldots, A_{132}) \leftarrow (t_3, A_1, A_2, \ldots, A_{68})\)
5. \((B_1, B_2, B_3, \ldots, B_{105}) \leftarrow (t_1, B_1, B_2, \ldots, B_{41})\)
6. \((C_1, C_2, C_3, \ldots, C_{147}) \leftarrow (t_2, C_1, C_2, \ldots, A_{83})\)
7. \( t = A_{[3\ldots66]} \oplus A_{[69\ldots132]} \oplus B_{[6\ldots69]} \oplus B_{[42\ldots105]} \oplus C_{[3\ldots66]} \oplus C_{[84\ldots147]} \oplus A_{[39\ldots102]} \land B_{[3\ldots66]} \)
**Circuit for VPV-Hash**

```
<table>
<thead>
<tr>
<th>K</th>
<th>32</th>
</tr>
</thead>
<tbody>
<tr>
<td>K'</td>
<td>32</td>
</tr>
</tbody>
</table>

MUX

64

32

VHorner_{64/4}

D/M D'/M'

32

64

256

VHorner_{32/5}

16

32

160

32 Bit Multiplier

16

64

256

Avik Chakraborti, Mridul Nandi

Important Features and Flexibilities of TriviA
Circuit for VPV-Hash

Main components of VPV-Hash

- Two V-Horner circuits (linear) of 64 and 32-bit operations.
- V-Horner basically consists of multiplications by primitive elements.
- One 32-bit field multiplier.
Work Flow for TriviA

- SC-TriviA
- State
- AD
- VPV-Hash
- Intermediate Value
- SC-TriviA
- State
- Encryption Key Stream
- Authentication Key Stream
- M
- C
- T

Avik Chakraborti, Mridul Nandi

Important Features and Flexibilities of TriviA
Work Flow for TriviA

Work Flow

- VPV-Hash processes AD to produce Intermediate data.
- The Intermediate data is XOR-ed with SC-TriviA state.
- SC-TriviA is reinitialized.
- Ensures change in AD changes the key stream.

Computation in One Clock-Cycle (64-bit message/AD is processed)

1. One 32 bit field multiplier.
2. Two V-Horner linear operations.
3. SC-TriviA state update and key generation.
## Security Level for TriviA

<table>
<thead>
<tr>
<th>Version</th>
<th>Confidentiality</th>
<th>Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>TriviA-0</td>
<td>128</td>
<td>126</td>
</tr>
<tr>
<td>TriviA-128</td>
<td>128</td>
<td>126</td>
</tr>
</tbody>
</table>
Suppose nonce can repeat up to \( n \) times. However, nonce together with AD should not repeat.

**Theorem: Privacy of TriviA**

\[
\text{Adv}_{\text{TriviA}}^{\text{priv}}(A) \leq \eta + \frac{qn}{2^{160}}.
\]

where \( \eta \) denotes the maximum distinguishing advantage over all adversaries \( B \) making at most \( \sigma \) block queries to Trivia-SC and running in time \( T_0 \) (which is about time of the adversary \( A \) plus some insignificant overhead).

**Theorem: Authenticity of TriviA**

\[
\text{Adv}_{\text{TriviA}}^{\text{auth}}(A) \leq \eta + \frac{qn}{2^{160}} + \frac{q}{2^{126}}.
\]
1. **TriviA AE Scheme**

2. **Features of TriviA**

3. **Possible Proposed Modification of TriviA**
**Important Properties of TriviA**

- Presence of Intermediate Tag.
- SC-TriviA - Updated design of a well studied and efficient (both in hardware and software) stream cipher Trivium.
- VPV-Hash - Low hardware area with minimum multiplications (Nandi, FSE 2014).
- Encryption and authentication key - Generated parallelly.
- High bit security- 128-bits for both confidentiality and integrity of plaintext.
1 TriviA AE Scheme

2 Features of TriviA

3 Possible Proposed Modification of TriviA
Motivation

- Construction of an extremely efficient AE scheme for lightweight devices.
- Lower the hardware area.
- Increase the Throughput.

Two Techniques of Updation

- Reduction of blocksize to perform 16-bit field multiplication.
- Removal of the encoding operation from the VPV-Hash.
**Motivation**

- Less hardware area $\Rightarrow$ More efficient in lightweight device.

- Major hardware area taken by VPV-Hash.
- Modification in VPV-Hash.
- No Change in SC-TriviA.
Reduce the Blocksize

- Process message in blocks of size 32 bits instead of 64-bits.
- Perform two 16-bit field multiplications instead of one 32-bit multiplication to process 64-bit in a clock cycle.
- The hardware area is reduced (Two 16-bit field multiplier takes less area than one 32-bit).
Removal of the Encode Operation

- VPV-Hash uses encode hash and combine technique.
- Removal of the encode operation doesn’t change security.
- Decreases the hardware area previously needed for the encoding.
Thank You

Any Questions?