# Important Features and Flexibilities of TriviA

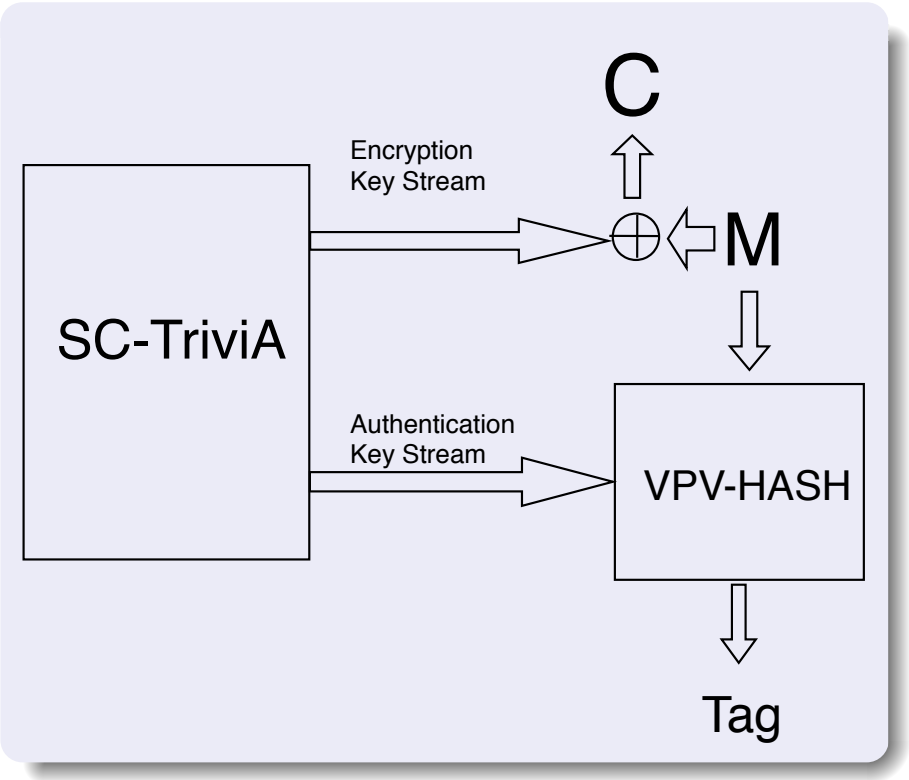
Avik Chakraborti, Mridul Nandi

Indian Statistical Institute, Kolkata

August 24, 2014
DIAC, UCSB

# Outline

# 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 - $\mathbb{F}_{2^{32}}$ and $\mathbb{F}_{2^{64}}$
- Encrypts message by *One-Time-Pad*.
- Intermediate tag - Computed after each $ck$ blocks.
- Size of each of the tags - 128-bit

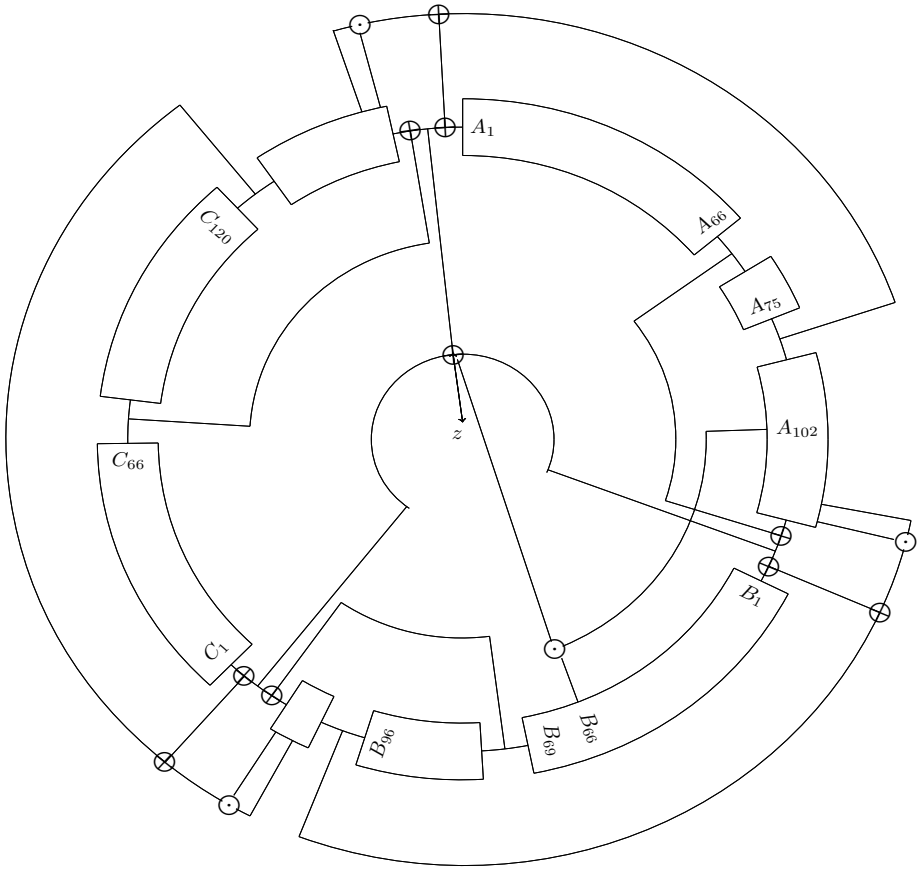
# Recommended Parameter Choice

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

## We recommend two versions

- TriviA-0 with $ck = 0$ and
- TriviA-128 with $ck = 128$

# SC-TriviA-Circuit



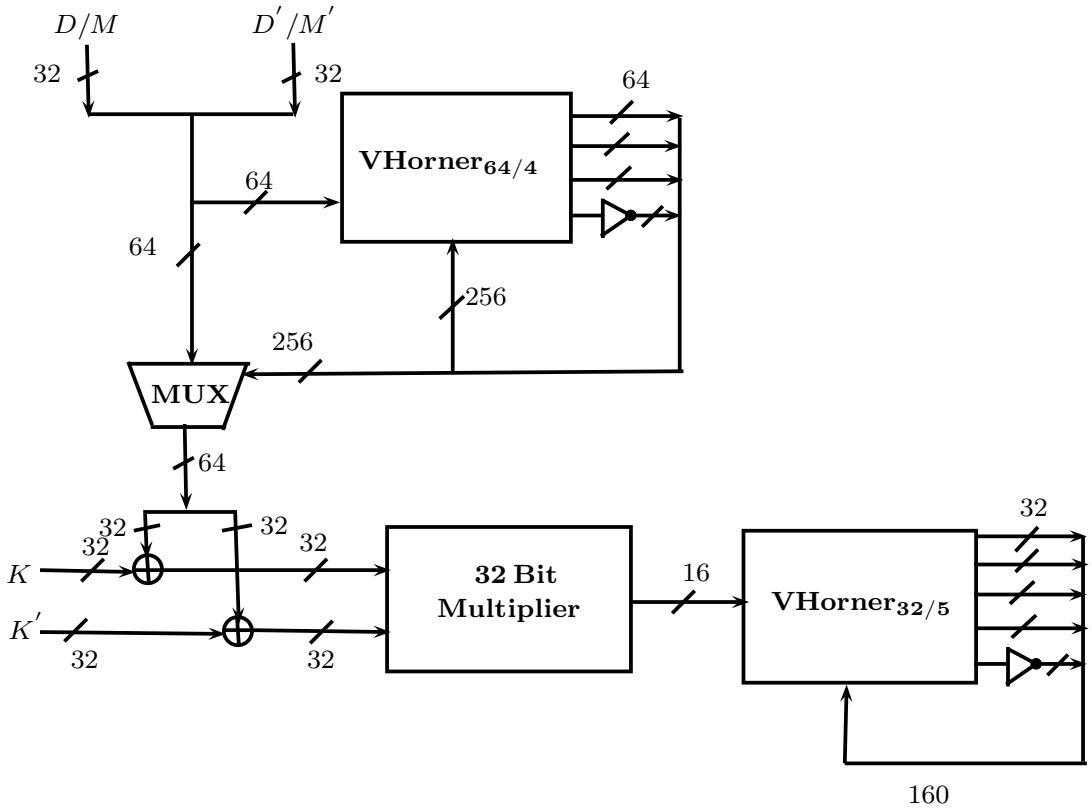

NFSR (nonlinear feedback): $|A| = 132, |B| = 105, |C| = 147.$

# Key Extraction and State Updation for SC-TriviA

## Key Extraction and State Updation for 64 rounds

1. $t_1 \leftarrow A_{[3\cdots66]} \oplus A_{[69\cdots132]} \oplus A_{[67\cdots130]} \wedge A_{[68\cdots131]} \oplus B_{[33\cdots96]}$
2. $t_2 \leftarrow B_{[6\cdots69]} \oplus B_{[42\cdots105]} \oplus B_{[40\cdots103]} \wedge B_{[41\cdots104]} \oplus C_{[57\cdots120]}$
3. $t_3 \leftarrow C_{[3\cdots66]} \oplus C_{[84\cdots147]} \oplus C_{[82\cdots145]} \wedge C_{[83\cdots146]} \oplus A_{[12\cdots75]}$
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. $\mathrm{t} = A_{[3\cdots66]} \oplus A_{[69\cdots132]} \oplus B_{[6\cdots69]} \oplus B_{[42\cdots105]} \oplus C_{[3\cdots66]} \oplus C_{[84\cdots147]} \oplus A_{[39\cdots102]} \wedge B_{[3\cdots66]}$

# Circuit for VPV-Hash

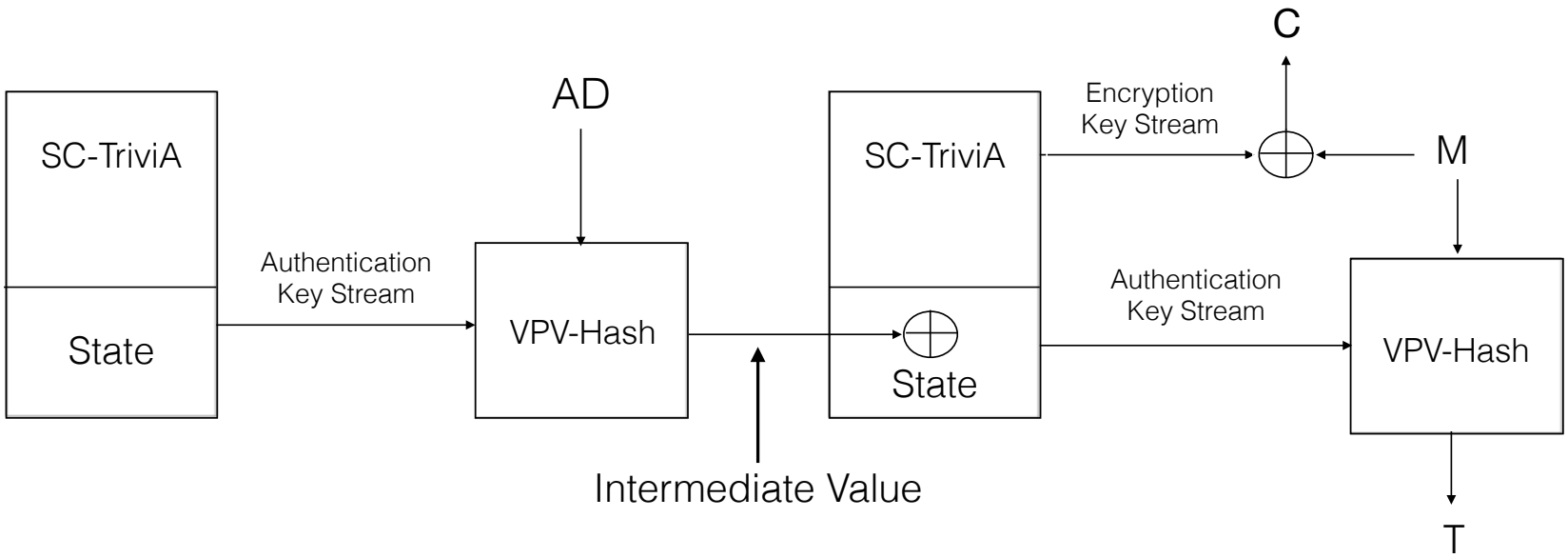


# Circuit for VPV-Hash

## 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



# 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

| Version | Confdentiality | Integrity |
|---|---|---|
| TriviA-0 | 128 | 126 |
| TriviA-128 | 128 | 126 |

# Security Theorems for TriviA

Suppose nonce can repeat up to $n$ times. However, nonce together with AD should not repeat.

## Theorem: Privacy of TriviA

$$\mathbf{Adv}^{\mathrm{priv}}_{TriviA}(A) \leq \eta + \frac{qn}{2^{160}}.$$

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

$$\mathbf{Adv}^{\mathrm{auth}}_{TriviA}(A) \leq \eta + \frac{qn}{2^{160}} + \frac{q}{2^{126}}.$$

# 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.

# Motivation

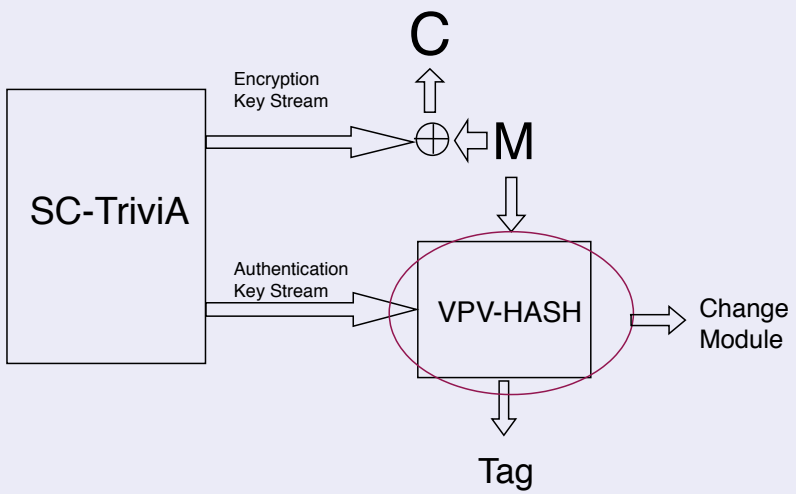
- Construction of an extremely efficient AE scheme for lightweight devices.
- Lower the hardware area.
- Increase the Throughput.

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?