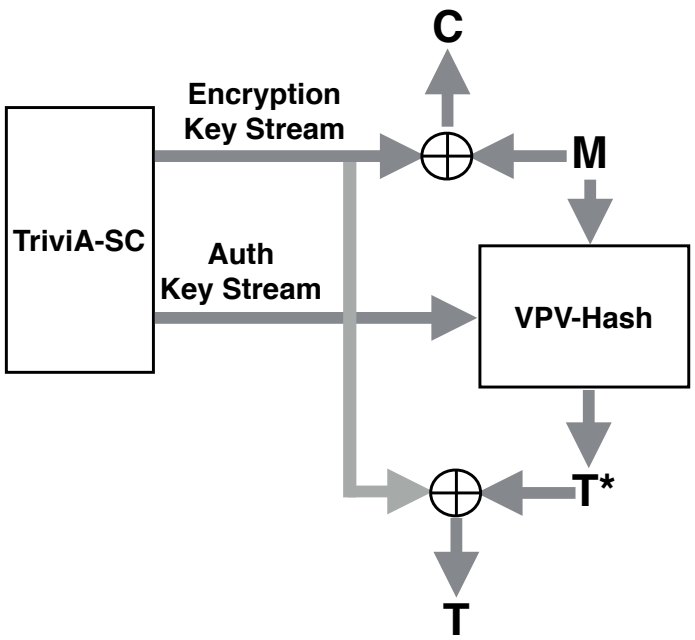
TriviA-ck-v2 : An Efficient Update of TriviA-ck-v1

Avik Chakraborti, Mridul Nandi

September 28, 2015

Outline of the talk

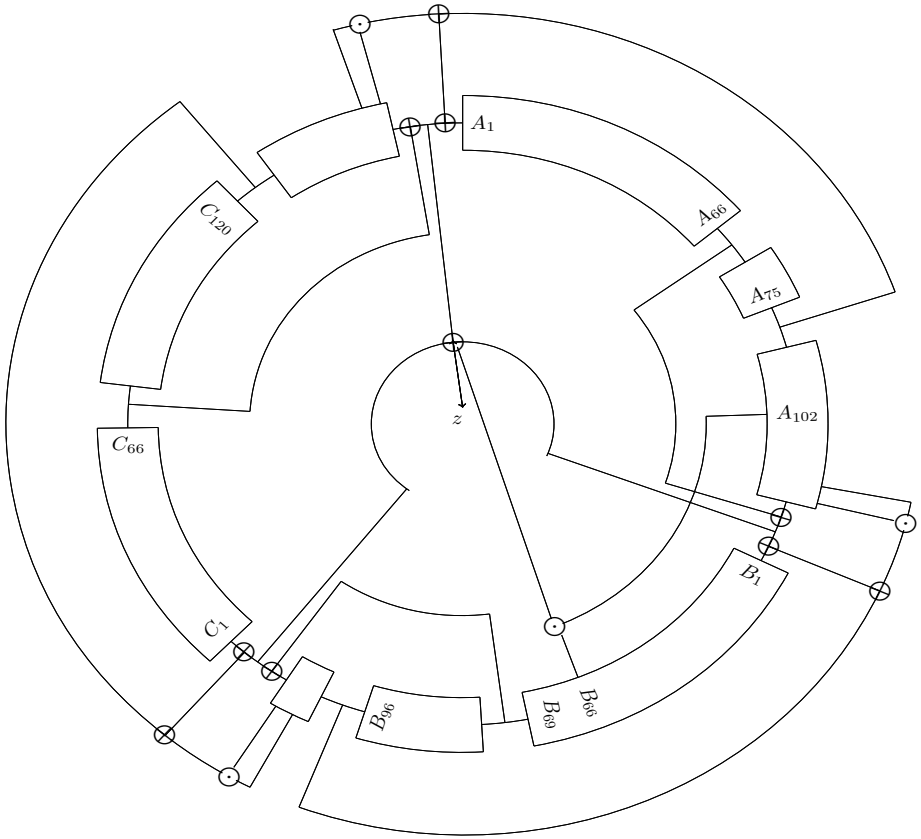
TriviA Encryption Mode



- TriviA-SC - Updated version of Trivium.
- VPV-Hash - Universal Hash follows EHC technique.
- TriviA-SC generates
  - *Encryption* key stream
  - *Authentication* key stream

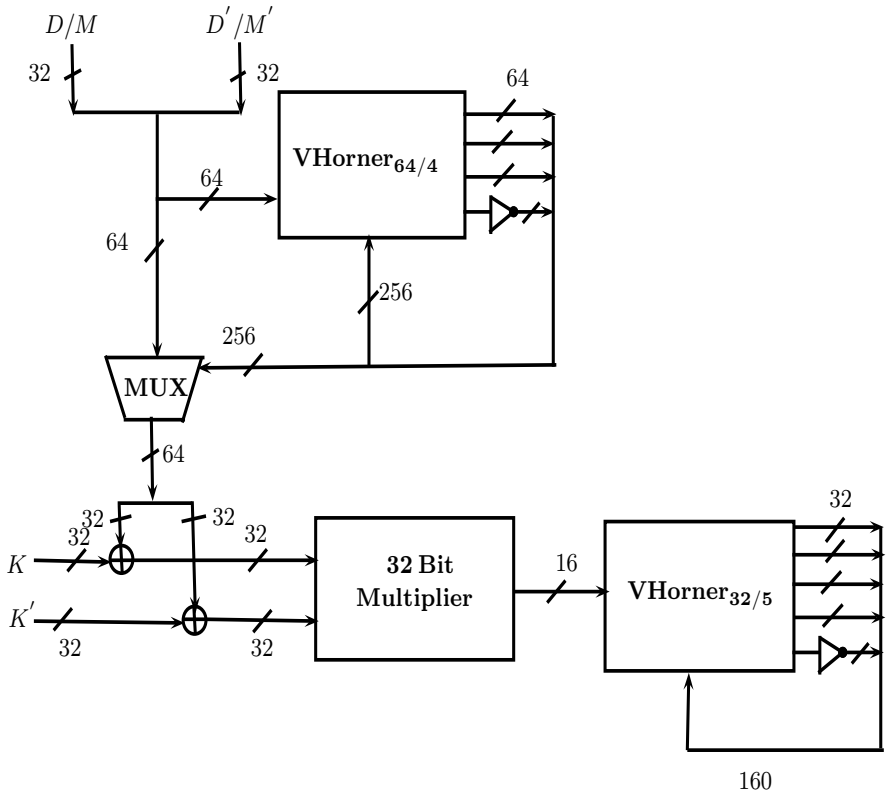
  parallely

A Trivium Based Stream Cipher : TriviA-SC



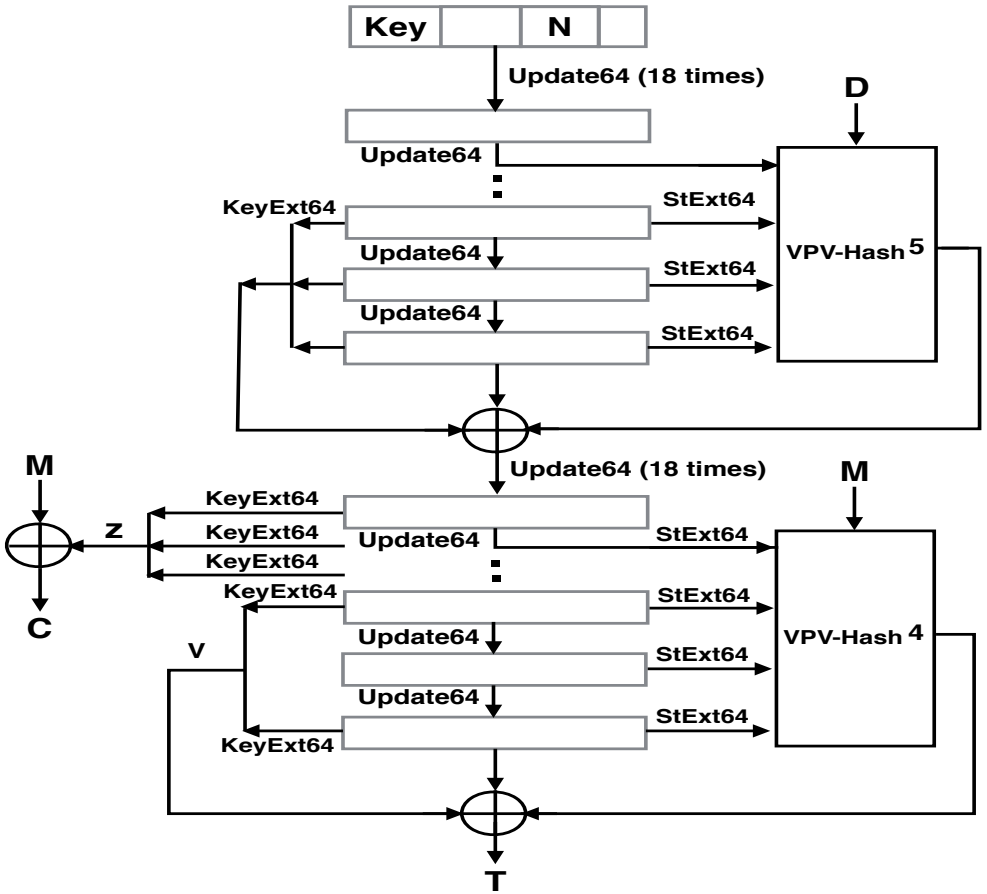
- Load 128-bit key, 128-bit nonce and *All One* constants

Circuit of VPV Hash



- ECCode$_d$ (VHorner$_{64/d}$) $\rightarrow$ PDP-Hash (32-bit Multiplier) $\rightarrow$ VMult$_{\alpha,d}$ (VHorner$_{32/d+1}$)

Lower Level Structure of TriviA



Updates of TriviA-ck-v1

Changes inside TriviA-SC

- Load TriviA-SC with all 0 except three bits

Changes in TriviA-ck-v1 Mode

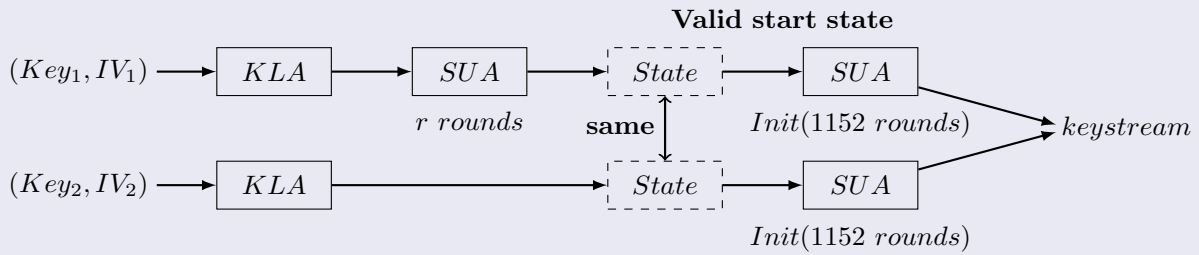
- Reduce Intermediate state from 160 to 128 bit

Changes inside VPV-Hash

- Reorder input and key block in PDP-Hash
- Add Variable Key in an Online manner

Updates in TriviA-SC

Slide Attack on TriviA-ck-v1



Solution

- Load fixed bits by 0 except for $B_{103}, B_{104}, B_{105}$ (with 1)
- Algebraic properties are similar as older SC

Changes in TriviA-ck-v1 Mode

- Intermediate state size $|T|$ is reduced from 160-bit to 128-bit
- Uses VPV^4 instead of VPV^5
- Both AD and M processing phase are symmetric
- Nonce should be distinct for each query

In VPV Hash : Reorder Input and Key Block in PDP Hash

- Parse $K = k_1||k_2||k_3||k_4$ and $x = x_1||x_2||x_3||x_4$
- $\mathrm{PDP}^*(K, x) = ((x_1||x_3) \oplus (k_1||k_3))((x_2||x_4) \oplus (k_2||k_4))$
- More Efficient field multilication in 32 bit platform

Efficiency of Multiplication in 32-bit Platform

First Clock Cycle

- $C_1 = (x_1 \oplus k_1)(x_2 \oplus k_2)$ (16-bit poly mult)
- Store $C_1.x^{16} \oplus C_1$, $(x_1 \oplus k_1)$ and $(x_2 \oplus k_2)$

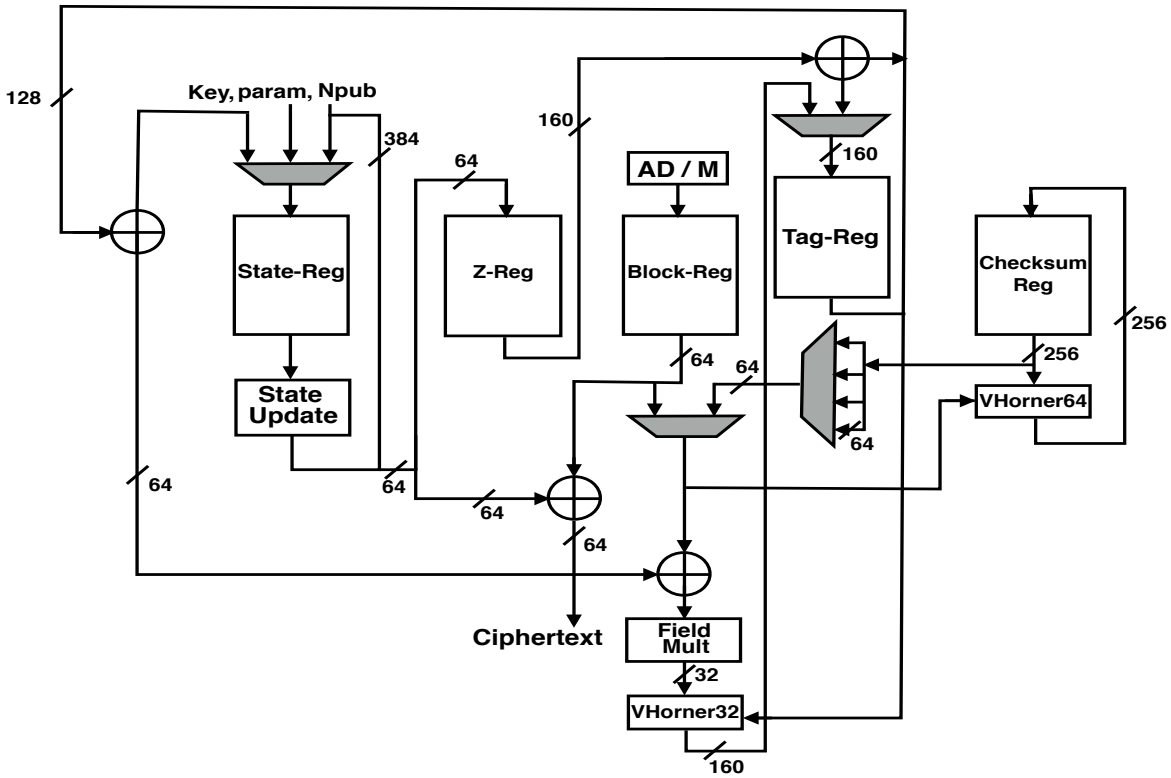
Second Clock Cycle

- $C_2 = ((x_1 \oplus k_1) \oplus (x_3 \oplus k_3))((x_2 \oplus k_2) \oplus (x_4 \oplus k_4))$
- $C_3 = (x_3 \oplus k_3)(x_4 \oplus k_4)$
- $out = (C_1' \oplus C_2 \oplus C_3).x^{16} \oplus C_3$

In VPV Hash : Changes in the Variable Key Addition Method

- Online addition of the 64-bit stream cipher output (first / second 64 bit variable key) with the intermediate state/ tag
- No need for separate register to store the variable key
- Maintains the pairwise independence property of VPV- Hash
- Multiply the 2^{nd} component of the variable key by α^2

Base Hardware Circuit for TriviA-ck-v1



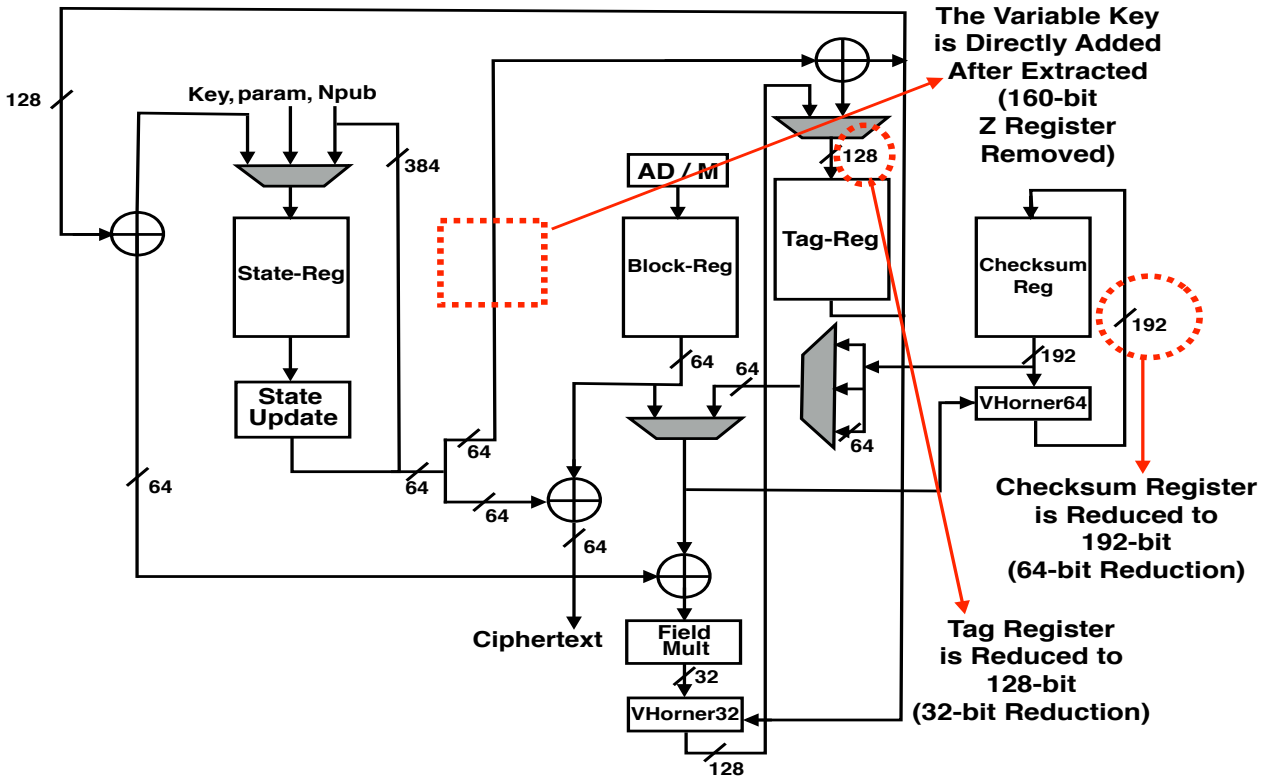
TriviA-ck-v1 ASIC Implementation

- Verilog HDL, Synopsys Design Compiler J-2014.09
- Technology node: UMC 65nm logic SP/RVT Low-K process

- Base Implementation
  - Area : 23.6 KGE
  - Frequency : 1150 MHZ, Throughput : 73.9 Gbps

- Another Pipelined Implementation (To increase throughput)
  - Area : 24.4 KGE
  - Frequency : 1425 MHZ, Throughput : 91.2 Gbps

Circuit for TriviA-ck-v2



Circuit for TriviA-ck-v2

- Mainly register storage can be reduced
- 96 bit reduced by intermediate state reduction
- 160 bit reduced by new variable key addition technique
- $1500 - 1800$ GE reduced (1-bit reg $\equiv 6 - 7$ GEs)

Conclusions and Future Works

- Four changes from triviA-ck-v1
- Reduces storage, faster *field mult* in 32-bit platform
- Reduces gate count
- Future Work
  - Hardware simulation of TriviA-ck-v2

Thank you