Signal Dictionary

ChaCha20 Stream Cipher Block Function & Block Counter Implementation

Complete Signal Reference as of 25/5/2025

Signal Classification Legend

Type	Color Code	Description
INPUT	Green	External inputs to modules
OUTPUT	Red	Module outputs
INTERNAL	Orange	Internal signals and registers

ChaCha State Matrix Module (ChaChaState)

Signal Name	Width	Type	Description
clk	1 bit	IN	System clock signal for synchronous operations
clrMatrix	1 bit	IN	Active high reset signal to clear the ChaCha matrix
Key[0:7]	256-bit (8 × 32-bit)	IN	256-bit encryption key split into 8 words (32-bit each)
Nonce[2:0]	96-bit (3 × 32-bit)	IN	96-bit nonce value split into 3 words (32-bit each)
Block	32-bit	IN	32-bit block counter for multi-block encryption
Constant[3:0]	128-bit (4 × 32-bit)	IN	128-bit ChaCha20 constants ("expand 32-byte k")
chachatoQround 4x4	512 (16 × 32-bit)	OUT	4×4 matrix of 32-bit words forming initial ChaCha state

Quarter-Round Processing Module (PerformQround)

Signal Name	Width	Type	Description
chachamatrixIN[3:0][3:0]	512-bit (16 × 32-bit)	IN	Input 4×4 ChaCha state matrix from state module
clk	1 bit	IN	System clock for state machine synchronization
setRounds	1 bit	IN	Initialize signal to start quarter-round processing
chachamatrixOUT 4x4	(16 × 32-bit)	OUT	Final processed 4×4 matrix after 20 rounds
Internal Signals			
INITchachastate 4x4	(16 × 32-bit)	INT	Copy of initial state for final addition step
TEMPchachastate 4x4	(16 × 32-bit)	INT	Temporary state during quarter-round processing
a, b, c, d	128-bit (4 × 32-bit each)	INT	Working registers for quarter-round operations
loadvalues	1 bit	INT	Control signal for loading matrix values into a,b,c,d

Signal Name	Width	Type	Description
CurrQ	3 bits	INT	Current quarter-round selector (Q0–Q7)
NextQ	3 bits	INT	Next quarter-round selector
Currstep	3 bits	INT	Current step in quarter-round state machine (S0–S7)
Nextstep	3 bits	INT	Next step in quarter-round state machine
counter	32-bit	INT	Round counter tracking completion of 20 rounds

Block Counter Module (Block_Counter)

Signal Name	Width	Type	Description
clk	1 bit	IN	System clock for counter synchronization
init	1 bit	IN	Initialize counter to zero
blocksproduced[B-1:0]	B bits (parameterized)	IN	Number of blocks produced
Block	32-bit	OUT	Current block counter value

State Machine Encodings

Quarter-Round State Machine (Currstep/Nextstep)

State	Encoding	Operation
S0	3'b000	a = a + b; d = d $\oplus$ (a + b)
S1	3'b001	c = c + d; d = d $\ll$ 16
S2	3'b010	b = b $\oplus$ c; d = d $\oplus$ a
S3	3'b011	b = b $\ll$ 12; d = d $\ll$ 16
S4	3'b100	a = a + b; d = d $\ll$ 8
S5	3'b101	c = c + d; d = d $\ll$ 7
S6	3'b110	b = b $\oplus$ c
S7	3'b111	Advance to next quarter-round

Quarter-Round Selector (CurrQ/NextQ)

State	Matrix Elements	Description
Q0	(0,0), (1,0), (2,0), (3,0)	Column 0 quarter-round
Q1	(0,1), (1,1), (2,1), (3,1)	Column 1 quarter-round
Q2	(0,2), (1,2), (2,2), (3,2)	Column 2 quarter-round
Q3	(0,3), (1,3), (2,3), (3,3)	Column 3 quarter-round
Q4	(0,0), (1,1), (2,2), (3,3)	Diagonal quarter-round
Q5	(1,0), (2,1), (3,2), (0,3)	Diagonal quarter-round
Q6	(2,0), (3,1), (0,2), (1,3)	Diagonal quarter-round
Q7	(3,0), (0,1), (1,2), (2,3)	Diagonal quarter-round

Critical Timing Relationships

- **Clock-to-Q Delay:** Time between clock edge and data output stabilization.
- **Setup Time:** Minimum time data must be stable before the clock edge.
- **Hold Time:** Minimum time data must remain stable after the clock edge.
- **Reset Recovery:** Clear signals must fully reset internal registers and state machines before reinitialization.
- **Propagation Delay:** Time taken for signals to propagate through combinational logic.

Signal Dictionary

Block Counter & State Matrix Modules

Signal Classification Legend

Type	Color Code	Description
INPUT	Green	External inputs to modules
OUTPUT	Red	Module outputs
INTERNAL	Orange	Internal signals and registers
PARAMETER	Purple	Module parameters

Block Counter Module (Block_Counter)

Module Parameters

Parameter	Default	Type	Description
B	4	param	Bit width of blocksproduced input signal

Port Signals

Signal Name	Width	Type	Description
clk	1	IN	System clock for counter synchronization
init	1	IN	Active high initialization signal to reset counter to zero
blocksproduced[B-1:0]	B	IN	Number of blocks produced (parameterized width, default 4-bit)
Block	32	OUT	Current block counter value (word_t typedef)

Functional Description

- **Counter Operation**: Increments by 1 each clock cycle when not in init mode
- **Reset Behavior**: When init is asserted, Block output is cleared to all zeros
- **Data Type**: Uses word_t typedef (32-bit logic vector)
- **Increment Value**: Fixed 4-bit increment (4'b1) regardless of parameter B

ChaCha State Matrix Module (ChaChaState)

Port Signals

Signal Name	Width	Type	Description
clk	1	IN	System clock signal for synchronous state matrix formation
clrMatrix	1	IN	Active high clear signal to reset entire ChaCha matrix to zero
Key[0:7]	32×8	IN	256-bit encryption key as array of 8 words (32-bit each)

Signal Name	Width	Type	Description
Nonce[2:0]	32×3	IN	96-bit nonce value as array of 3 words (32-bit each)
Block	32	IN	32-bit block counter value from Block_Counter module
Constant[3:0]	32×4	IN	128-bit ChaCha20 constants as array of 4 words
chachatoQround 4x4	32×16	OUT	Complete 4×4 ChaCha state matrix for quarter-round processing

Matrix Layout & Mapping

Row	[0]	[1]	[2]	[3]
0	Constant[0]	Constant[1]	Constant[2]	Constant[3]
1	Key[0]	Key[1]	Key[2]	Key[3]
2	Key[4]	Key[5]	Key[6]	Key[7]
3	Block	Nonce[0]	Nonce[1]	Nonce[2]

Key Mapping Algorithm

The key mapping uses integer arithmetic for systematic placement:

- **Row Calculation**: `1 + j/4` where j is key index (0-7)
- **Column Calculation**: `j%4` where j is key index (0-7)
- **Result**: Key[0-3] → Row 1, Key[4-7] → Row 2

Inter-Module Connectivity

Data Flow Between Modules

Source Module	Output Signal	Dest. Module	Input Signal
Block_Counter	Block[31:0]	ChaChaState	Block[31:0]
ChaChaState	MToQround	PerformQround	chachamatrixIN[3:0][3:0]

Synchronization Requirements

- **Clock Domain**: All modules operate on same clock domain
- **Reset Sequencing**: Block_Counter init should precede ChaChaState clrMatrix
- **Data Validity**: Block counter output must stabilize before matrix formation
- **Pipeline Timing**: State matrix formation takes 1 clock cycle after inputs valid

Implementation Notes

ChaCha20 Standard Compliance

- **Constants**: Typically "expand 32-byte k" (0x61707865, 0x3320646e, 0x79622d32, 0x6b206574)
- **Key Size**: 256-bit key as specified in RFC 8439
- **Nonce Size**: 96-bit nonce for ChaCha20 variant
- **Block Counter**: 32-bit counter allows $2^{32} \times 64$ bytes = 256GB per key/nonce pair

Synthesis Considerations

- **Register Usage**: 16 × 32-bit registers for state matrix + 32-bit counter
- **Logic Resources**: Minimal combinational logic, primarily data routing
- **Timing**: Single cycle latency for state matrix formation
- **Reset Strategy**: Synchronous reset recommended for FPGA implementation