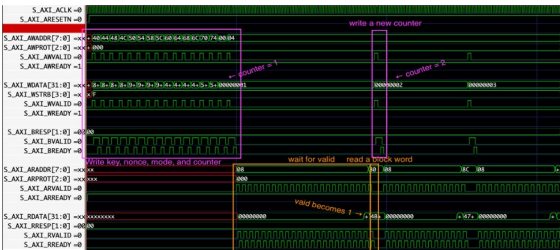




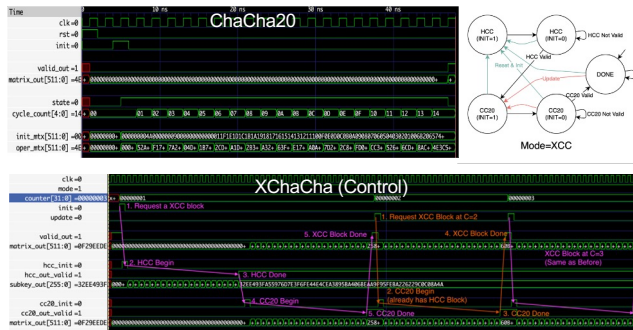
Semester Goals

- ### CPU Integration Progress

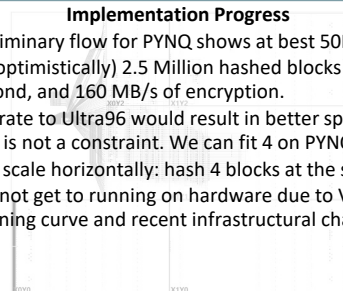
-
- The diagram illustrates the hardware interconnection between a ZYNQ Processing System and an HSC miniAid_0 module. On the left, the ZYNQ Processing System is shown with various peripheral interfaces: USB2.0, SPI, I2C, and multiple UARTs (UART0, UART1, UART2, UART3, UART4, UART5, UART6, UART7, UART8, UART9, UART10, UART11, UART12, UART13, UART14, UART15, UART16, UART17, UART18, UART19, UART20, UART21, UART22, UART23, UART24, UART25, UART26, UART27, UART28, UART29, UART30, UART31, UART32, UART33, UART34, UART35, UART36, UART37, UART38, UART39, UART40, UART41, UART42, UART43, UART44, UART45, UART46, UART47, UART48, UART49, UART50, UART51, UART52, UART53, UART54, UART55, UART56, UART57, UART58, UART59, UART60, UART61, UART62, UART63, UART64, UART65, UART66, UART67, UART68, UART69, UART70, UART71, UART72, UART73, UART74, UART75, UART76, UART77, UART78, UART79, UART80, UART81, UART82, UART83, UART84, UART85, UART86, UART87, UART88, UART89, UART90, UART91, UART92, UART93, UART94, UART95, UART96, UART97, UART98, UART99, UART100, UART101, UART102, UART103, UART104, UART105, UART106, UART107, UART108, UART109, UART110, UART111, UART112, UART113, UART114, UART115, UART116, UART117, UART118, UART119, UART120, UART121, UART122, UART123, UART124, UART125, UART126, UART127, UART128, UART129, UART130, UART131, UART132, UART133, UART134, UART135, UART136, UART137, UART138, UART139, UART140, UART141, UART142, UART143, UART144, UART145, UART146, UART147, UART148, UART149, UART150, UART151, UART152, UART153, UART154, UART155, UART156, UART157, UART158, UART159, UART160, UART161, UART162, UART163, UART164, UART165, UART166, UART167, UART168, UART169, UART170, UART171, UART172, UART173, UART174, UART175, UART176, UART177, UART178, UART179, UART180, UART181, UART182, UART183, UART184, UART185, UART186, UART187, UART188, UART189, UART190, UART191, UART192, UART193, UART194, UART195, UART196, UART197, UART198, UART199, UART200, UART201, UART202, UART203, UART204, UART205, UART206, UART207, UART208, UART209, UART210, UART211, UART212, UART213, UART214, UART215, UART216, UART217, UART218, UART219, UART220, UART221, UART222, UART223, UART224, UART225, UART226, UART227, UART228, UART229, UART230, UART231, UART232, UART233, UART234, UART235, UART236, UART237, UART238, UART239, UART240, UART241, UART242, UART243, UART244, UART245, UART246, UART247, UART248, UART249, UART250, UART251, UART252, UART253, UART254, UART255, UART256, UART257, UART258, UART259, UART260, UART261, UART262, UART263, UART264, UART265, UART266, UART267, UART268, UART269, UART270, UART271, UART272, UART273, UART274, UART275, UART276, UART277, UART278, UART279, UART280, UART281, UART282, UART283, UART284, UART285, UART286, UART287, UART288, UART289, UART290, UART291, UART292, UART293, UART294, UART295, UART296, UART297, UART298, UART299, UART300, UART301, UART302, UART303, UART304, UART305, UART306, UART307, UART308, UART309, UART310, UART311, UART312, UART313, UART314, UART315, UART316, UART317, UART318, UART319, UART320, UART321, UART322, UART323, UART324, UART325, UART326, UART327, UART328, UART329, UART330, UART331, UART332, UART333, UART334, UART335, UART336, UART337, UART338, UART339, UART340, UART341, UART342, UART343, UART344, UART345, UART346, UART347, UART348, UART349, UART350, UART351, UART352, UART353, UART354, UART355, UART356, UART357, UART358, UART359, UART360, UART361, UART362, UART363, UART364, UART365, UART366, UART367, UART368, UART369, UART370, UART371, UART372, UART373, UART374, UART375, UART376, UART377, UART378, UART379, UART380, UART381, UART382, UART383, UART384, UART385, UART386, UART387, UART388, UART389, UART390, UART391, UART392, UART393, UART394, UART395, UART396, UART397, UART398, UART399, UART400, UART401, UART402, UART403, UART404, UART405, UART406, UART407, UART408, UART409, UART410, UART411, UART412, UART413, UART414, UART415, UART416, UART417, UART418, UART419, UART420, UART421, UART422, UART423, UART424, UART425, UART426, UART427, UART428, UART429, UART430, UART431, UART432, UART433, UART434, UART435, UART436, UART437, UART438, UART439, UART440, UART441, UART442, UART443, UART444, UART445, UART446, UART447, UART448, UART449, UART450, UART451, UART452, UART453, UART454, UART455, UART456, UART457, UART458, UART459, UART460, UART461, UART462, UART463, UART464, UART465, UART466, UART467, UART468, UART469, UART470, UART471, UART472, UART473, UART474, UART475, UART476, UART477, UART478, UART479, UART480, UART481, UART482, UART483, UART484, UART485, UART486, UART487, UART488, UART489, UART490, UART491, UART492, UART493, UART494, UART495, UART496, UART497, UART498, UART499, UART500, UART501, UART502, UART503, UART504, UART505, UART506, UART507, UART508, UART509, UART510, UART511, UART512, UART513, UART514, UART515, UART516, UART517, UART518, UART519, UART520, UART521, UART522, UART523, UART524, UART525, UART526, UART527, UART528, UART529, UART530, UART531, UART532, UART533, UART534, UART535, UART536, UART537, UART538, UART539, UART540, UART541, UART542, UART543, UART544, UART545, UART546, UART547, UART548, UART549, UART550, UART551, UART552, UART553, UART554, UART555, UART556, UART557, UART558, UART559, UART560, UART561, UART562, UART563, UART564, UART565, UART566, UART567, UART568, UART569, UART570, UART571, UART572, UART573, UART574, UART575, UART576, UART577, UART578, UART579, UART580, UART581, UART582, UART583, UART584, UART585, UART586, UART587, UART588, UART589, UART590, UART591, UART592, UART593, UART594, UART595, UART596, UART597, UART598, UART599, UART600, UART601, UART602, UART603, UART604, UART605, UART606, UART607, UART608, UART609, UART610, UART611, UART612, UART613, UART614, UART615, UART616, UART617, UART618, UART619, UART620, UART621, UART622, UART623, UART624, UART625, UART626, UART627, UART628, UART629, UART630, UART631, UART632, UART633, UART634, UART635, UART636, UART637, UART638, UART639, UART640, UART641, UART642, UART643, UART644, UART645, UART646, UART647, UART648, UART649, UART650, UART651, UART652, UART653, UART654, UART655, UART656, UART657, UART658, UART659, UART660, UART661, UART662, UART663, UART664, UART665, UART666, UART667, UART668, UART669, UART670, UART671, UART672, UART673, UART674, UART675, UART676, UART677, UART678, UART679, UART680, UART681, UART682, UART683, UART684, UART685, UART686, UART687, UART688, UART689, UART690, UART691, UART692, UART693, UART694, UART695, UART696, UART697, UART698, UART699, UART700, UART701, UART702, UART703, UART704, UART705, UART706, UART707, UART708, UART709, UART710, UART711, UART712, UART713, UART714, UART715, UART716, UART717, UART718, UART719, UART720, UART721, UART722, UART723, UART724, UART725, UART726, UART727, UART728, UART729, UART730, UART731, UART732, UART733, UART734, UART735, UART736, UART737, UART738, UART739, UART740, UART741, UART742, UART743, UART744, UART745, UART746, UART747, UART748, UART749, UART750, UART751, UART752, UART753, UART754, UART755, UART756, UART757, UART758, UART759, UART760, UART761, UART762, UART763, UART764, UART765, UART766, UART767, UART768, UART769, UART770, UART771, UART772, UART773, UART774, UART775, UART776, UART777, UART778, UART779, UART780, UART781, UART782, UART783, UART784, UART785, UART786, UART787, UART788, UART789, UART790, UART791, UART792, UART793, UART794, UART795, UART796, UART797, UART798, UART799, UART800, UART801, UART802, UART803, UART8



- Fixed ChaCha20 block function and verified it with publicly available test vectors.
- Implemented HChaCha block function and XChaCha control block function, and verified them against known test vectors.
- Made 11 tests for block function functional correctness
- Made 4 tests for correctness of control circuits
- Aesthetic and readability changes including the adoption of concise and readable packed arrays and other features from newer version of Verilog or SystemVerilog.



- Preliminary flow for PYNQ shows at best 50Mhz clock, or (optimistically) 2.5 Million hashed blocks per second, and 160 MB/s of encryption.
- Migrate to Ultra96 would result in better speed.
- Size is not a constraint. We can fit 4 on PYNQ fabric.
- Can scale horizontally: hash 4 blocks at the same time.
- Did not get to running on hardware due to Vivado learning curve and recent infrastructural changes.



Challenges and Lessons Learned

Challenges

- Repo from the previous semester was disorganized and needed fixing
- Having to rewrite the Verilog implementations
- Couldn't access any development VMs for a bit

Lessons Learned

- Verilog is now cleaner and more readable
- Learned how to properly containerize the design
- Proper documentation: New members should no longer have to start from scratch

Moving Forward

- Run on hardware. Easy now as implementation is mostly done.
- Speedup the existing design with faster busses, better FSM, and DSP optimized block functions.
- Improve onboarding & documentation, especially for students new to Verilog and FPGA.
- Formal Verification of the FSMs.

Containerization Progress

- Successful running of testbenches through the containerization of iverilog and vvp in both Docker and Apptainer.
- Automation of testing via Makefile.

```
VCD info: dumpfile tmp/trace/tb_xcc_block_func_mode_xcc.vcd opened for output.
[DONE] tb_xcc_block_func_mode_xcc.v: All 3 matrix matched after 91 clock cycles.
tb/tb_xcc_block_func_mode_xcc.v:146: $finish called at 192000 (1ps)
VCD info: dumpfile tmp/trace/tb_xcc_mnio_xcc_3wvds.vcd opened for output.
[DONE] tb_xcc_mnio_xcc_3wvds.v: All 3 matrix matched after 117 clock cycles.
tb/tb_xcc_mnio_xcc_3wvds.v:168: $finish called at 238000 (1ps)
root@a4129f15aa6:/v1p-reconfig-subteam/Desktop/Georgia Tech/Spring 2025/Future Computin
```