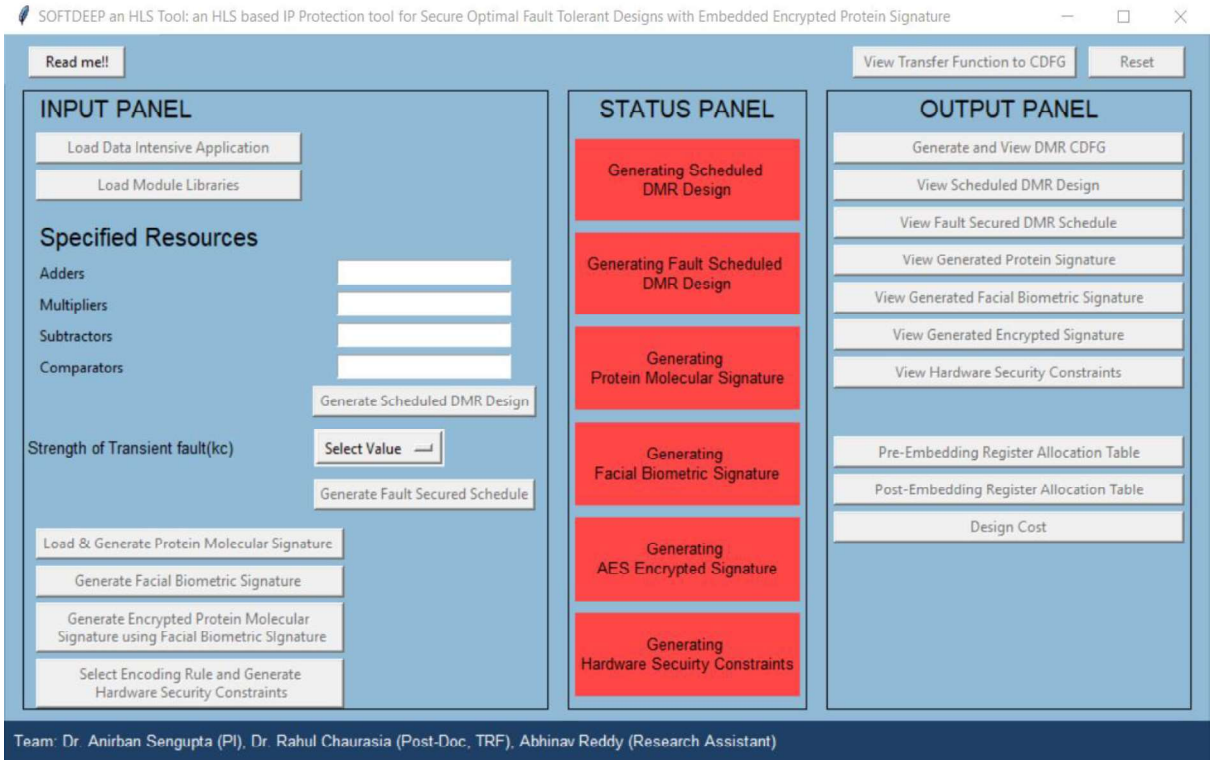
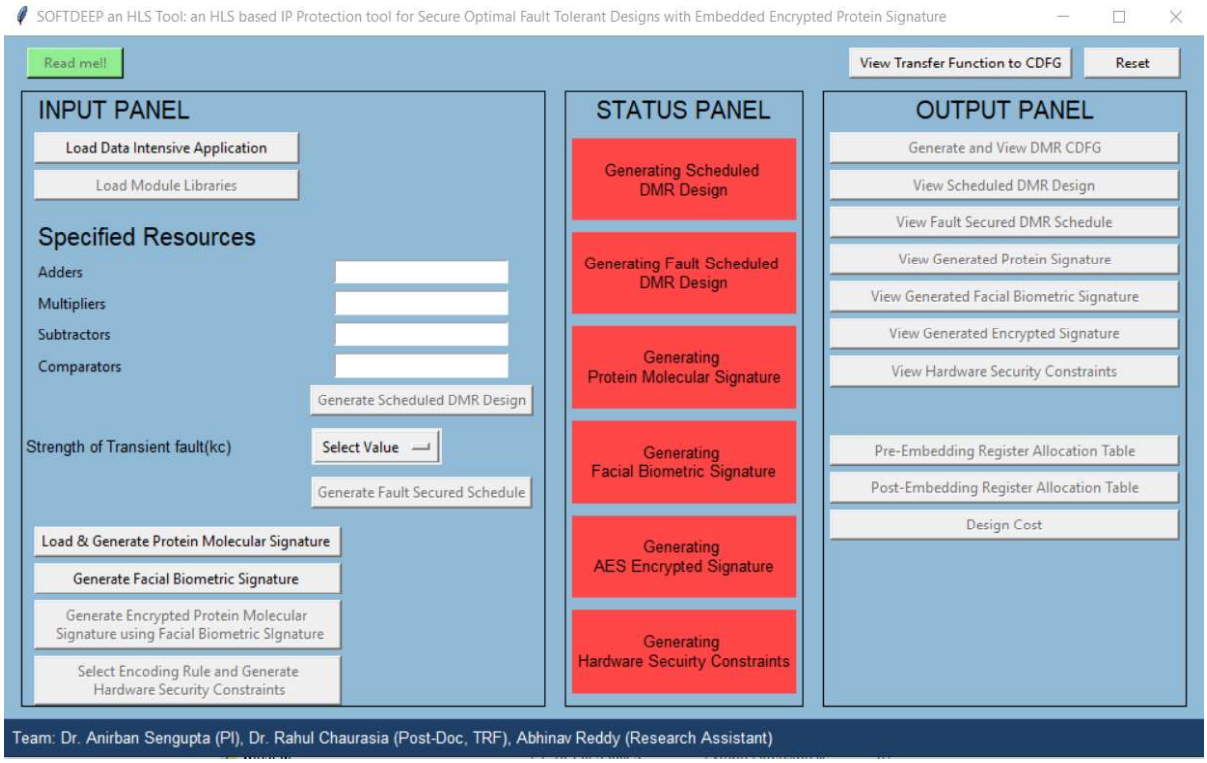
SOFTDEEP an HLS Tool: an HLS based IP Protection tool for **S**ecure **O**ptimal **F**ault **T**olerant **D**esigns with **E**mbedded **E**ncrypted **P**rotein **S**ignature

STEP-1: Run the tool→ Upon running the executable tool file, a display window appears as shown below. To activate the tool, user needs to click on the 'Read me!!' Tab. Thereafter a read me file opens up for user(s) that provides the summary and background of the tool and its attributes.

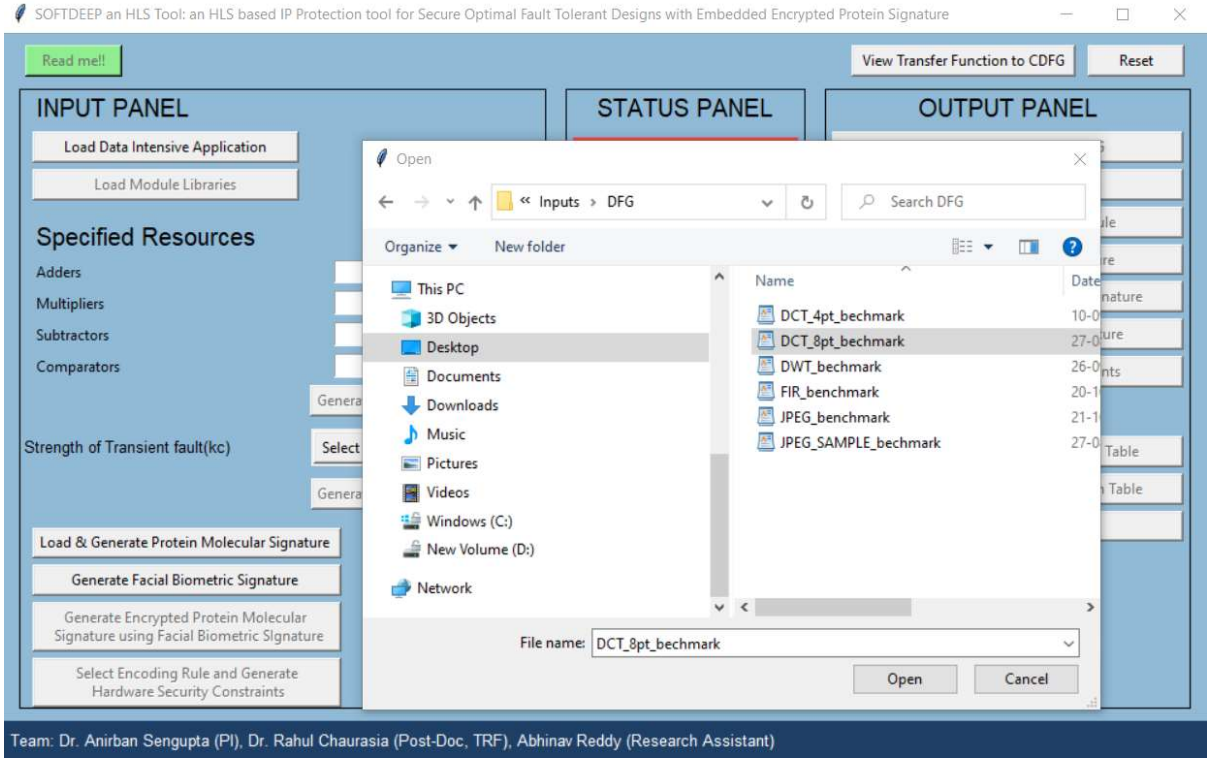


STEP-2: Post closing the read me file, the Tab 'Readme!!' turns GREEN and also the Tab 'Load Data Intensive Application' gets enabled. Further, two other independent module Tabs 'Load & Generate Protein Molecular Signature' and 'Generate Facial Biometric Signature' also gets enabled as shown below. Now user/IP vendor can access the 'INPUT PANEL' of the tool. Here user is asked to load data intensive application (sample application for which secure and optimal K-cycle fault detectable design with piracy detective control is to be generated).

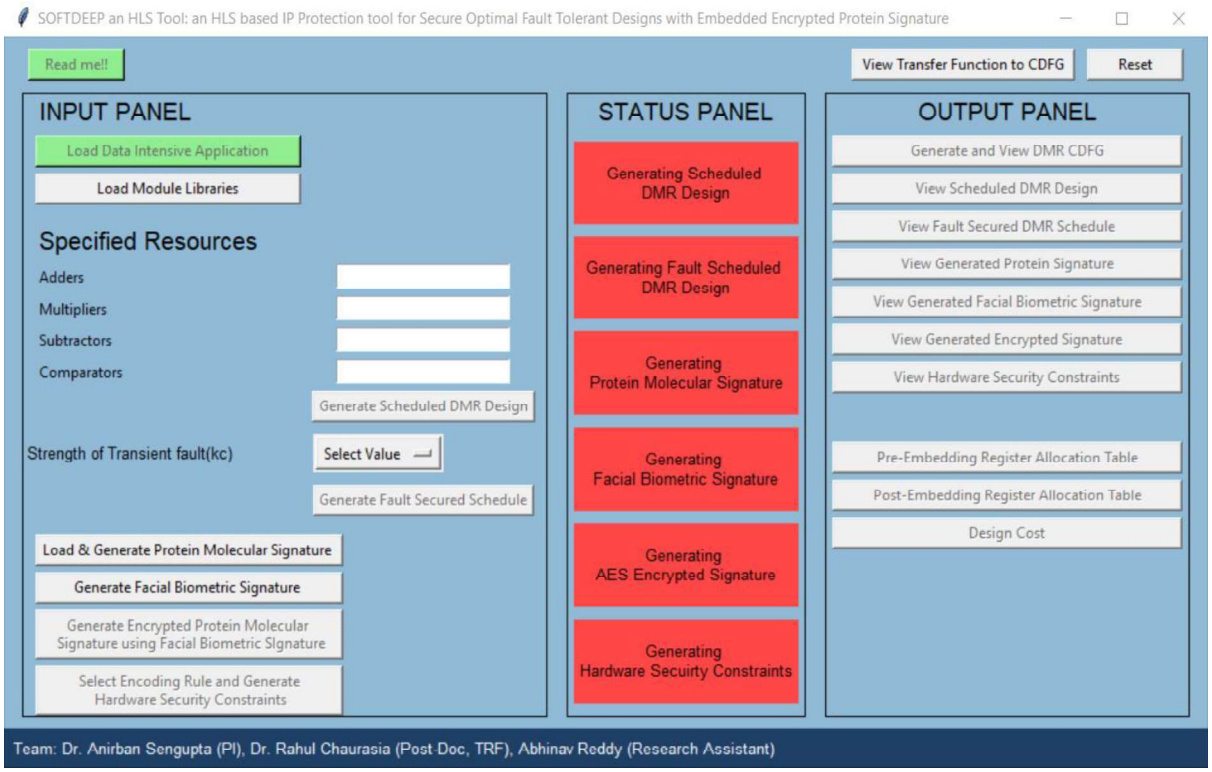


This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

→Post clicking on the Tab 'Load Data Intensive Application', a pop-up window appears for user (as shown below) to select the sample data intensive application, corresponding to which secure optimal K-cycle fault tolerant data path processor with embedded encrypted protein molecular biometric as piracy detective countermeasure is to be generated. *Note: For example, DCT_8pt_benchmak has been selected here*.

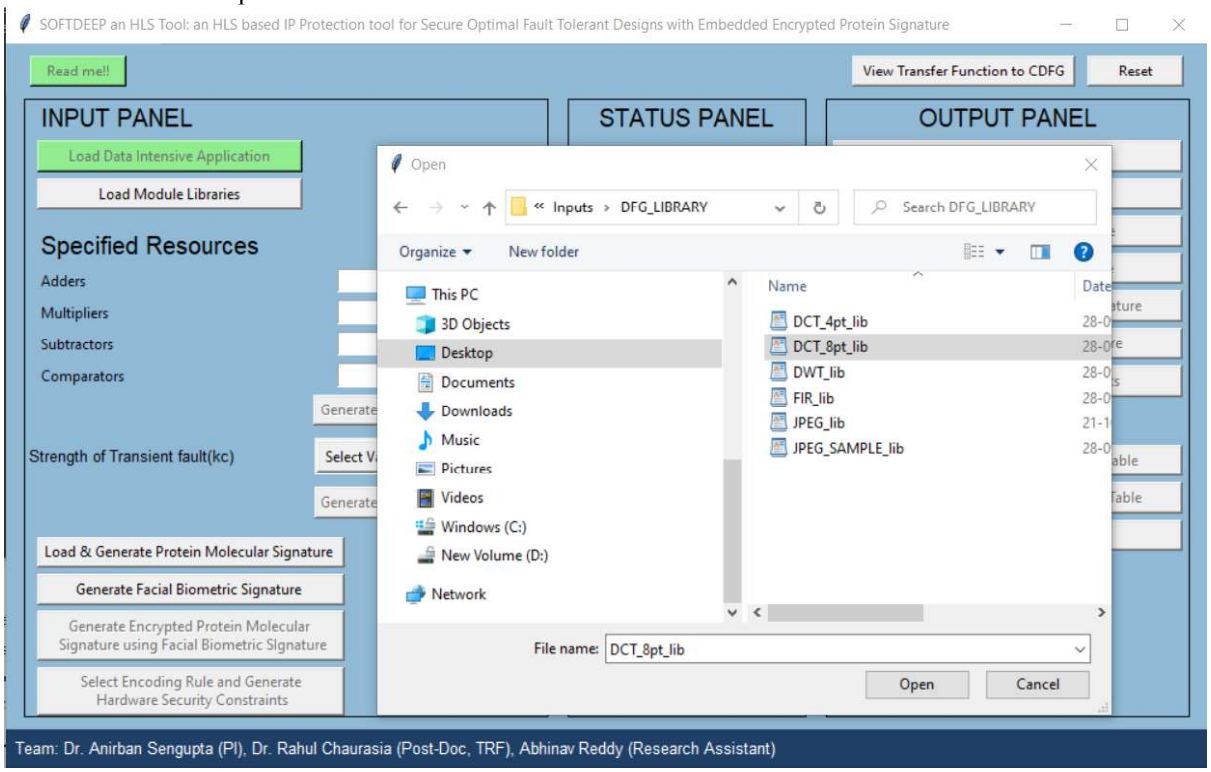


STEP-3: Post loading the sample data intensive application, its Tab turns GREEN and the Tab 'Load Module Libraries' gets enabled as shown below.

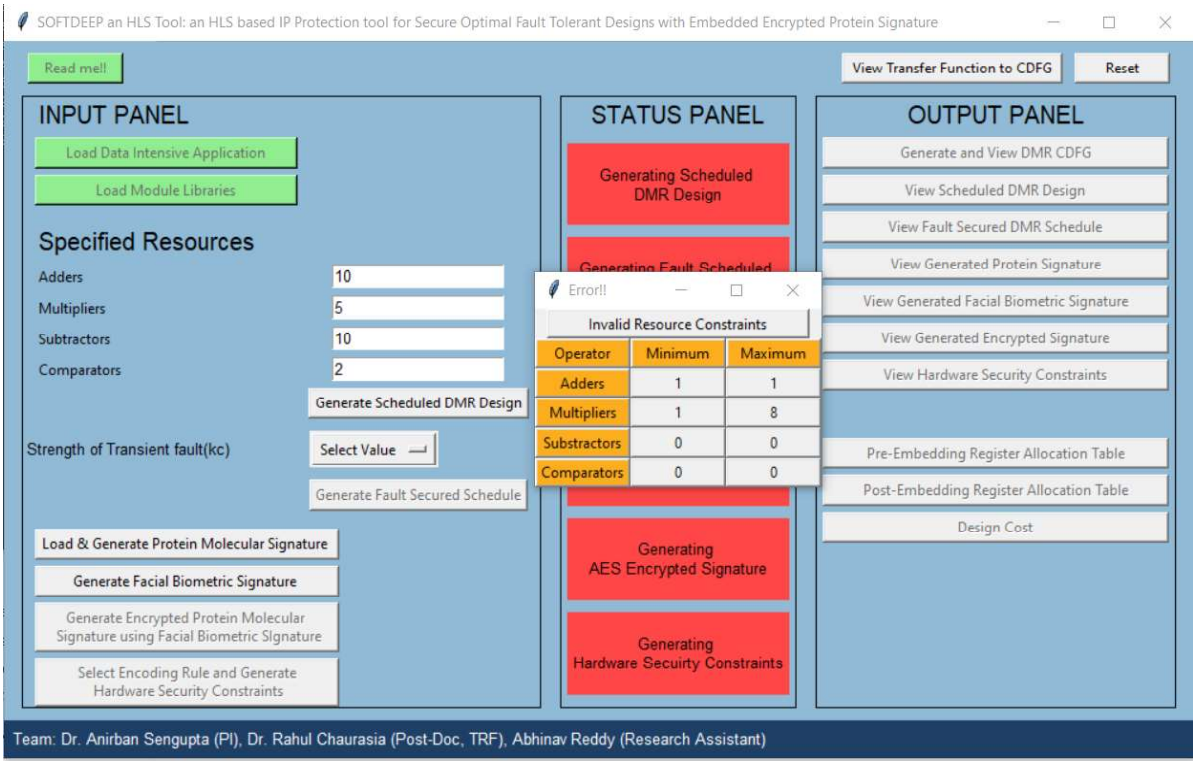


This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

→Next, the user is asked to load module libraries. By clicking the Tab 'Load Module Libraries' a pop-up window appears for user to select corresponding module library which comprises the details of hardware functional unit (FU) resources such as multipliers and adders/subtractors (in terms of area and latency of resources) and available hardware resources for allocation. *Note: For example, library corresponding to DCT_8pt_benchmak has been selected here*. The output screen is shown below:

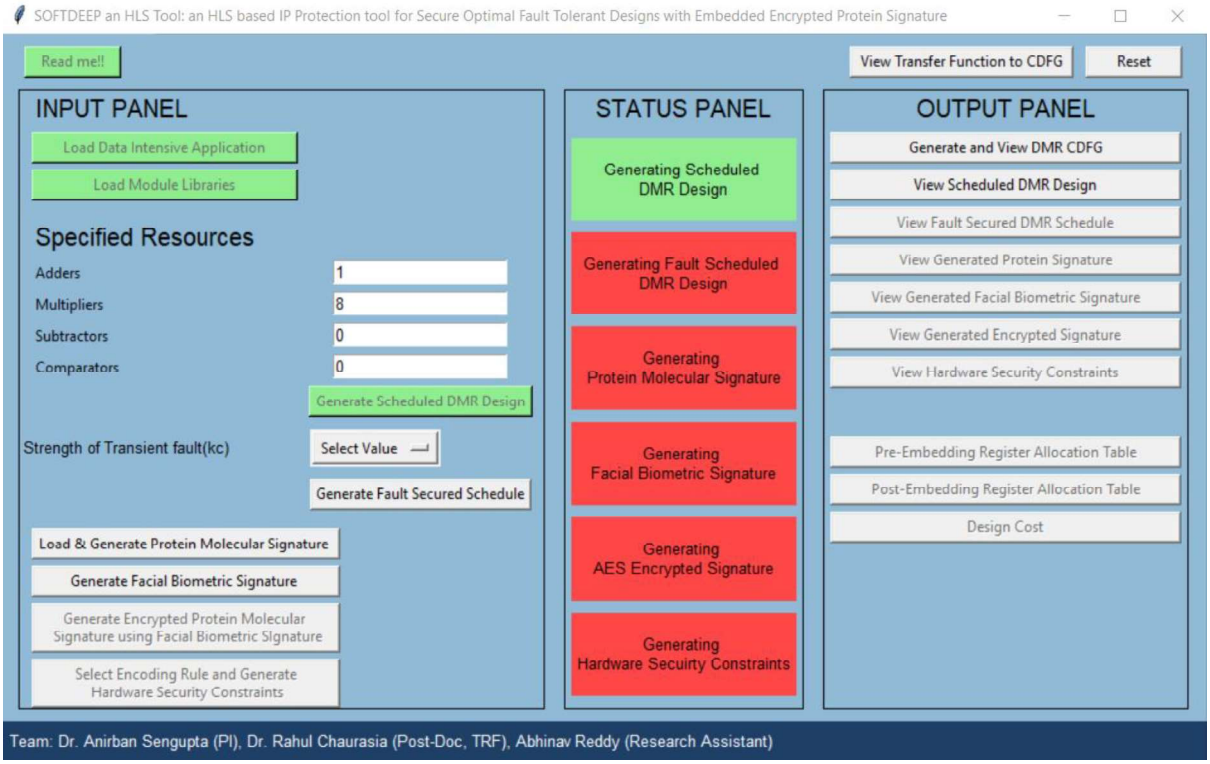


STEP-4: Post loading module library (15 nm open cell library) its Tab turns GREEN as shown below. Next, the user is asked to enter/specify the resources based on which design is to be scheduled/generated. *Note:* if user enters the resource configuration exceeding the limits of Min/Max available resources in the module library, then the tool throws an error saying 'Invalid Resource Constraints'. The output screen is shown below:

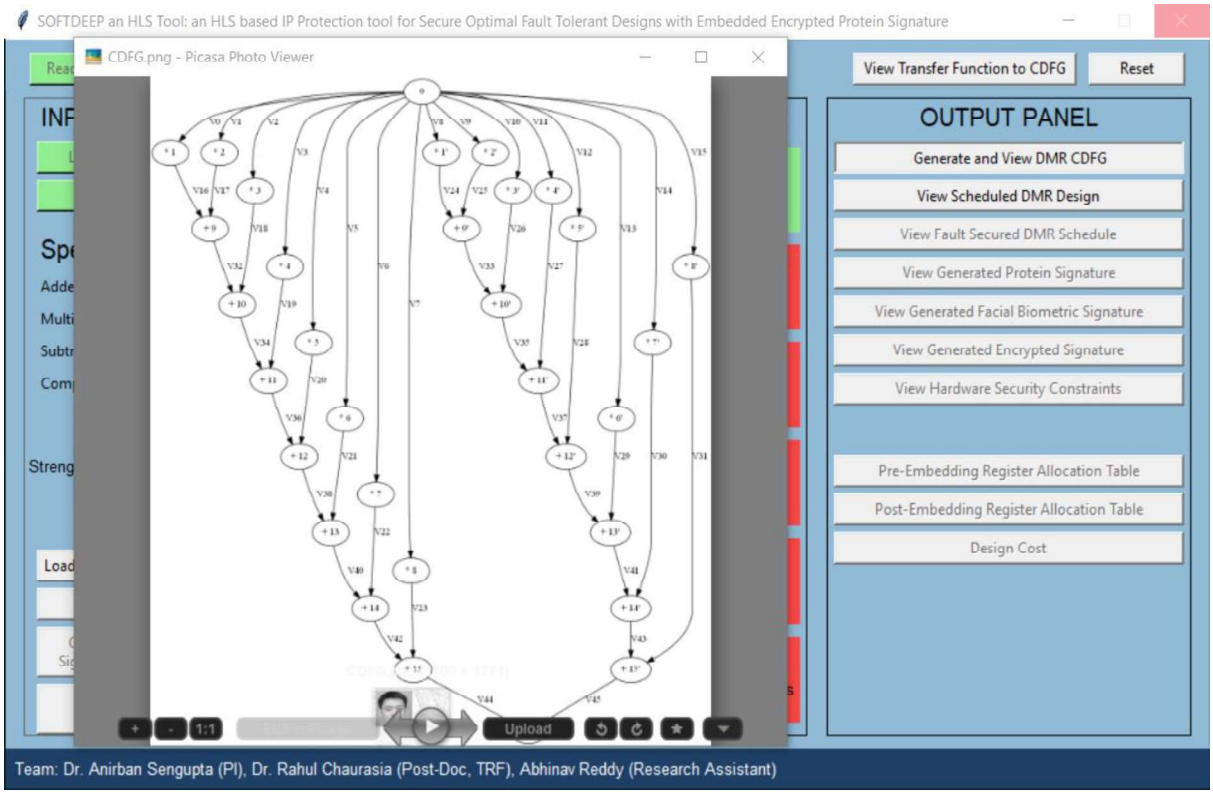


This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

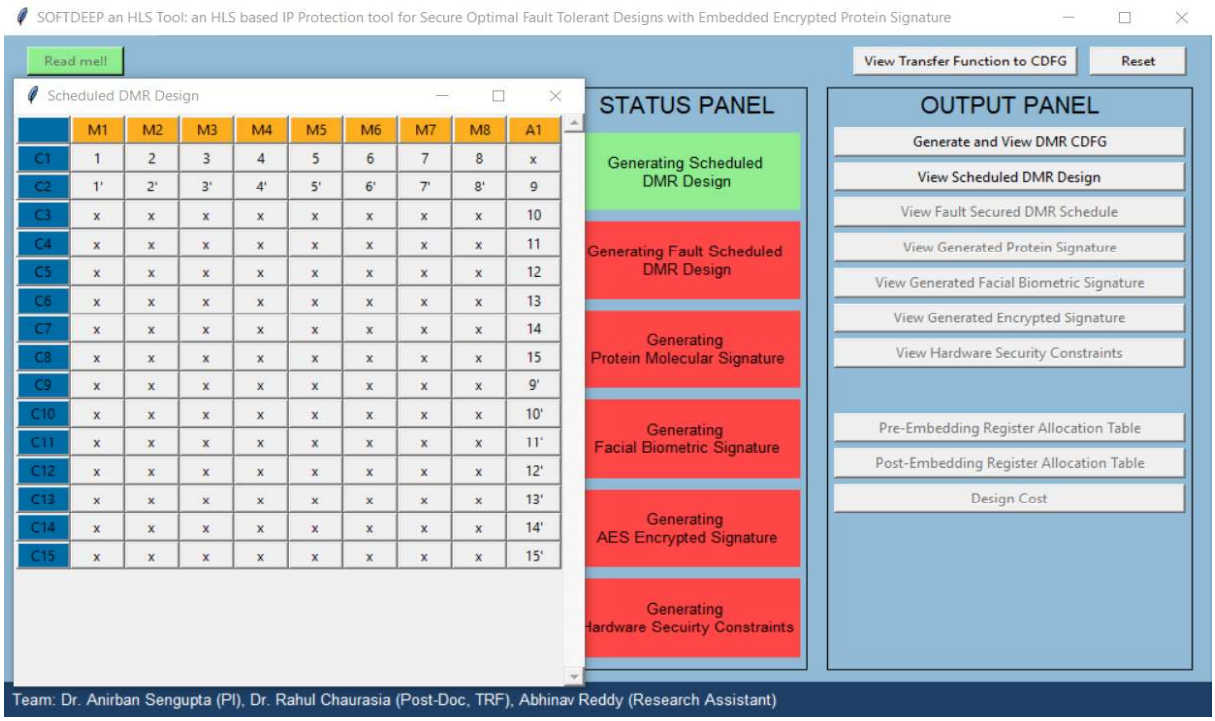
→Now, by entering the resources within the range, user can generate scheduled DMR design. **Post clicking on Tab** 'Generate scheduled DMR Design', the Tabs 'Generate and View DMR CDFG' and 'View Scheduled DMR Design' in the OUTPUT PANEL gets enabled and the status bar 'Generating Scheduled DMR Design' turns GREEN.



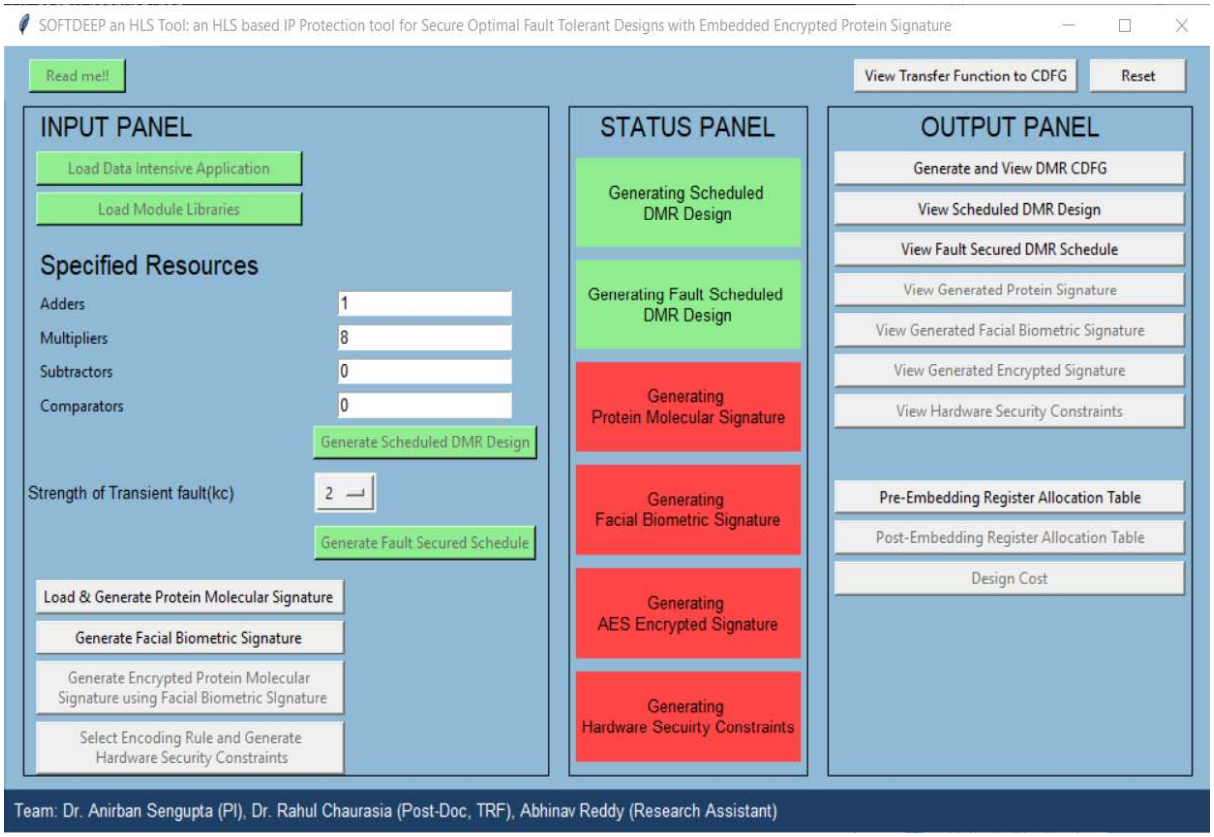
→User can view the generated 'DMR CDFG' and the scheduled DMR design (in the form of table) by clicking on it. The output screens are shown below:



This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

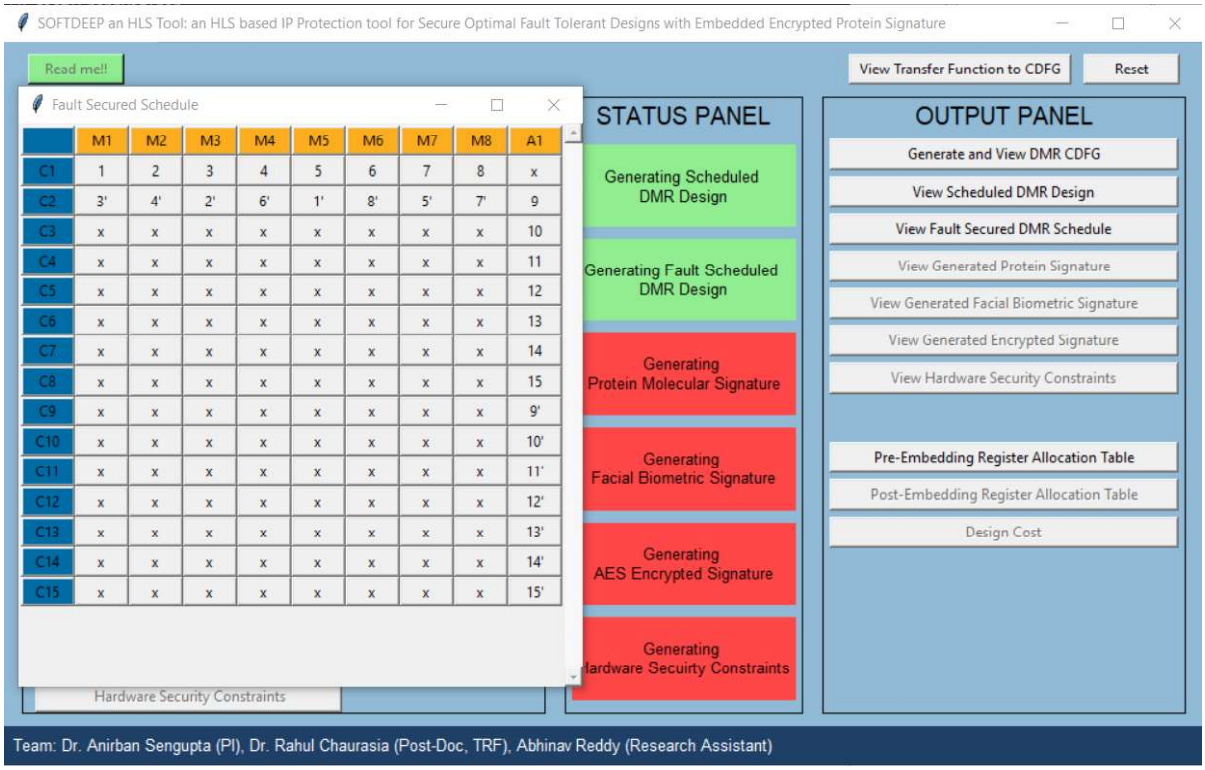


STEP-5: Next, user is asked to select strength of transient fault (considering in the range 1 to 3 for single/multi-cycle transient fault). Post selecting the strength of transient fault (e.g., Kc=2), user can generate fault secured schedule for the application. By clicking on Tab 'Generate Fault Secured Schedule' the Tab 'View Fault secured DMR schedule' and 'Pre-Embedding Register Allocation table' in the OUTPUT PANEL gets enabled and the tab 'Generating Fault Scheduled DMR Design' in the status bar turns GREEN as shown below:



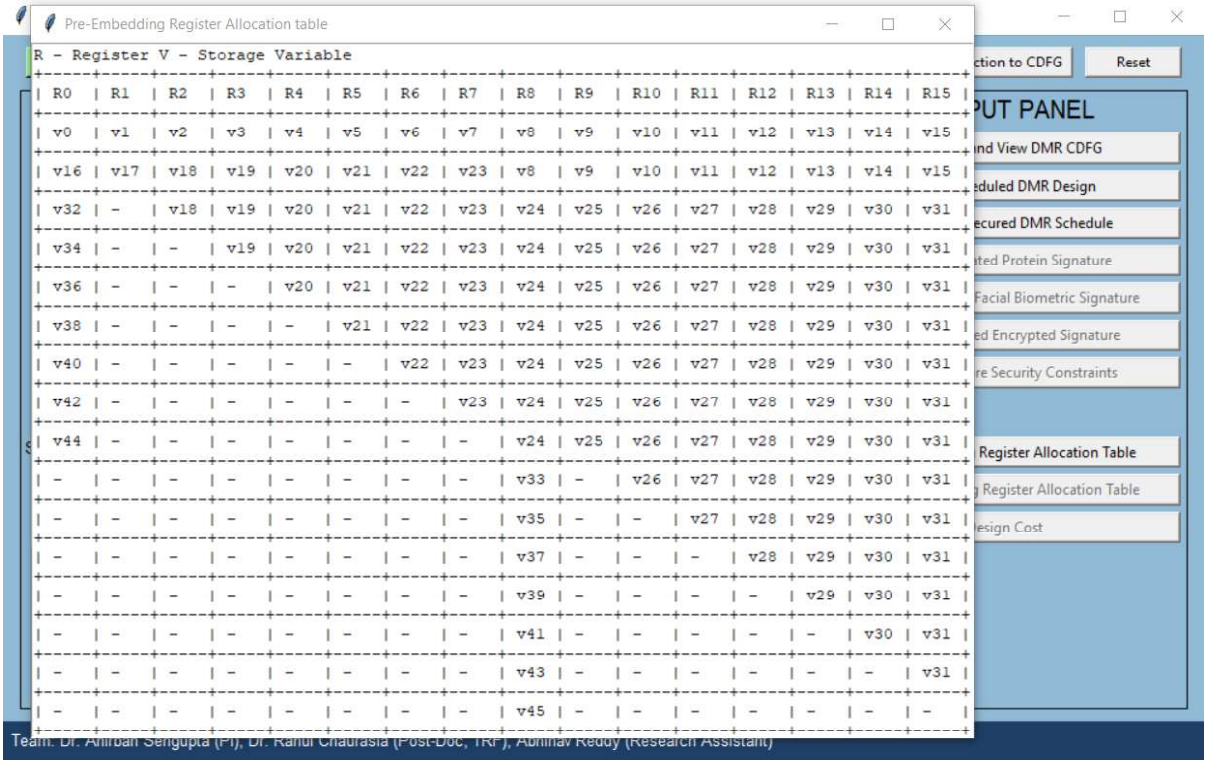
This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

→Now, user can view 'Fault Secured DMR Schedule' by clicking on the corresponding Tab. The output screen is shown below:



	M1	M2	M3	M4	M5	M6	M7	M8	A1
C1	1	2	3	4	5	6	7	8	x
C2	3'	4'	2'	6'	1'	8'	5'	7'	9
C3	x	x	x	x	x	x	x	x	10
C4	x	x	x	x	x	x	x	x	11
C5	x	x	x	x	x	x	x	x	12
C6	x	x	x	x	x	x	x	x	13
C7	x	x	x	x	x	x	x	x	14
C8	x	x	x	x	x	x	x	x	15
C9	x	x	x	x	x	x	x	x	9'
C10	x	x	x	x	x	x	x	x	10'
C11	x	x	x	x	x	x	x	x	11'
C12	x	x	x	x	x	x	x	x	12'
C13	x	x	x	x	x	x	x	x	13'
C14	x	x	x	x	x	x	x	x	14'
C15	x	x	x	x	x	x	x	x	15'

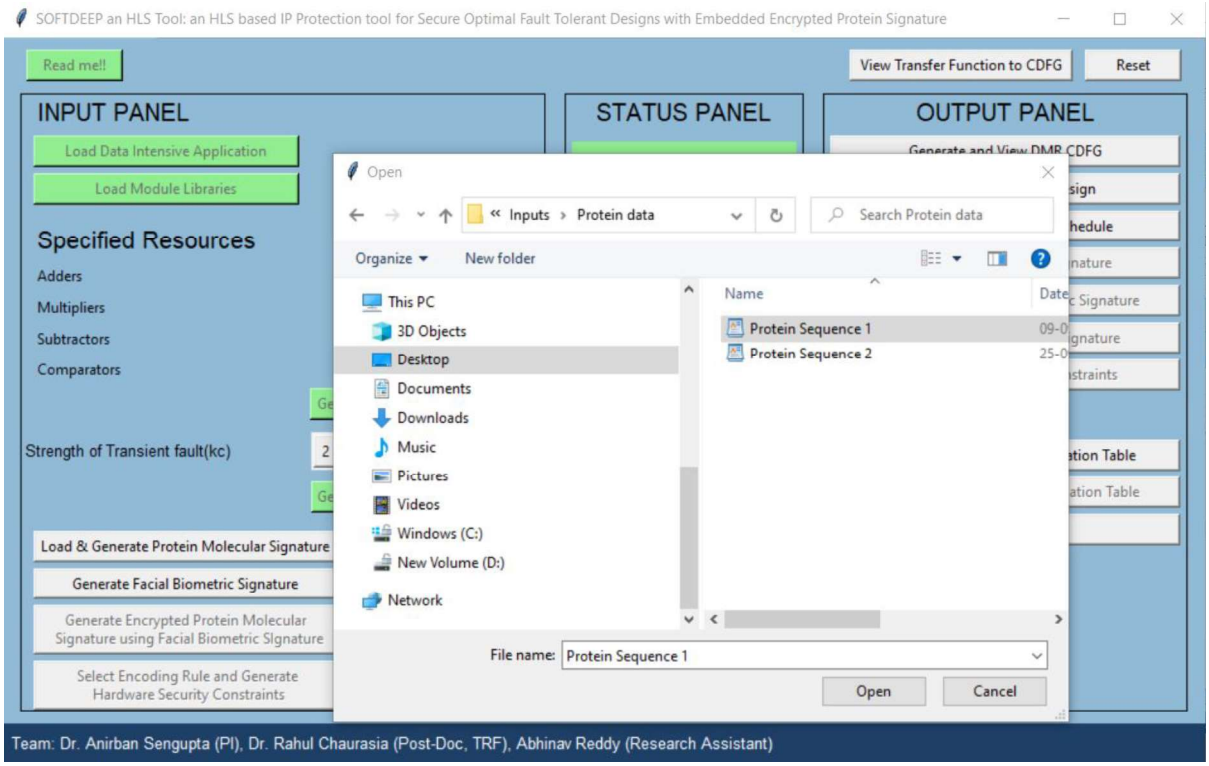
→Further, user can also view 'Pre-Embedding Register Allocation table' by clicking on it. The output screen is shown below:



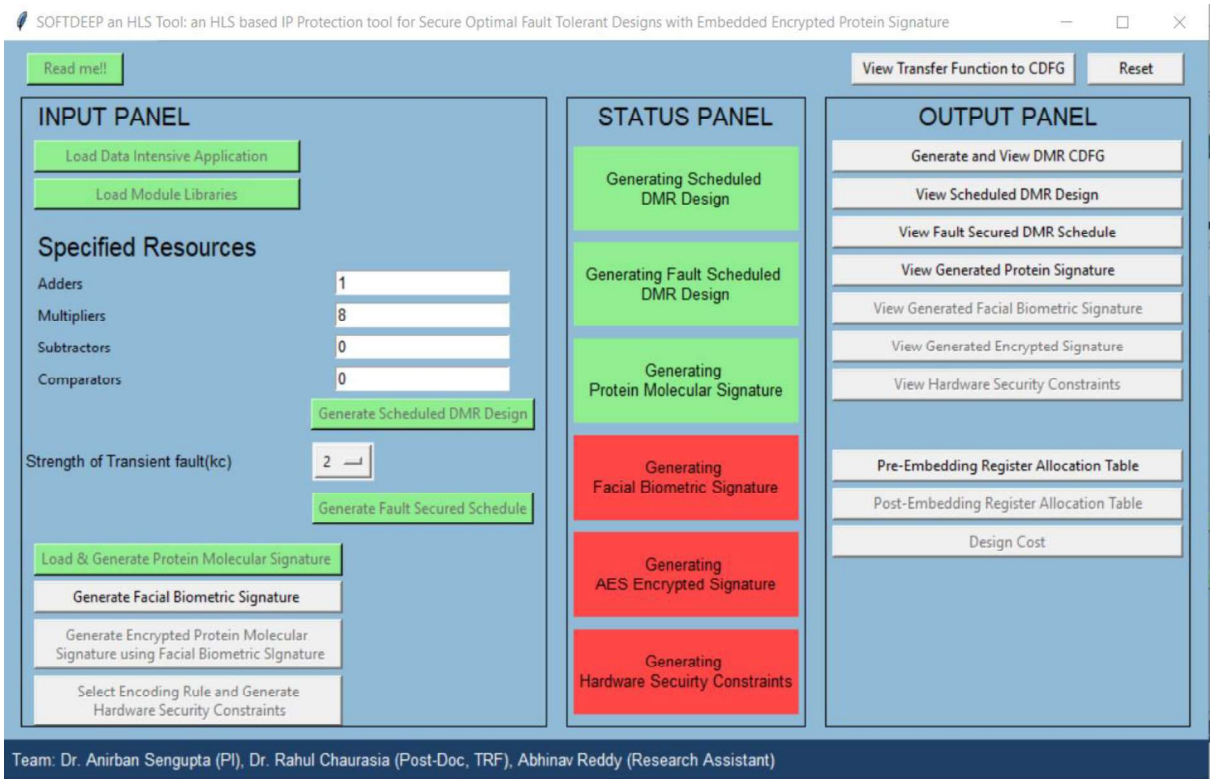
R0	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15
v0	v1	v2	v3	v4	v5	v6	v7	v8	v9	v10	v11	v12	v13	v14	v15
v16	v17	v18	v19	v20	v21	v22	v23	v8	v9	v10	v11	v12	v13	v14	v15
v32	-	v18	v19	v20	v21	v22	v23	v24	v25	v26	v27	v28	v29	v30	v31
v34	-	-	v19	v20	v21	v22	v23	v24	v25	v26	v27	v28	v29	v30	v31
v36	-	-	-	v20	v21	v22	v23	v24	v25	v26	v27	v28	v29	v30	v31
v38	-	-	-	-	v21	v22	v23	v24	v25	v26	v27	v28	v29	v30	v31
v40	-	-	-	-	-	v22	v23	v24	v25	v26	v27	v28	v29	v30	v31
v42	-	-	-	-	-	-	v23	v24	v25	v26	v27	v28	v29	v30	v31
v44	-	-	-	-	-	-	-	v24	v25	v26	v27	v28	v29	v30	v31
-	-	-	-	-	-	-	-	v33	-	v26	v27	v28	v29	v30	v31
-	-	-	-	-	-	-	-	v35	-	-	v27	v28	v29	v30	v31
-	-	-	-	-	-	-	-	v37	-	-	-	v28	v29	v30	v31
-	-	-	-	-	-	-	-	v39	-	-	-	-	v29	v30	v31
-	-	-	-	-	-	-	-	v41	-	-	-	-	-	v30	v31
-	-	-	-	-	-	-	-	v43	-	-	-	-	-	-	v31
-	-	-	-	-	-	-	-	v45	-	-	-	-	-	-	-

This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

STEP-6: Next, user is asked to load protein molecular sequence and generate protein molecular signature. By clicking the Tab 'Load & Generate Protein Molecular Signature' a pop-up window appears for user to select the protein sample of original IP vendor. The output screen is shown below:

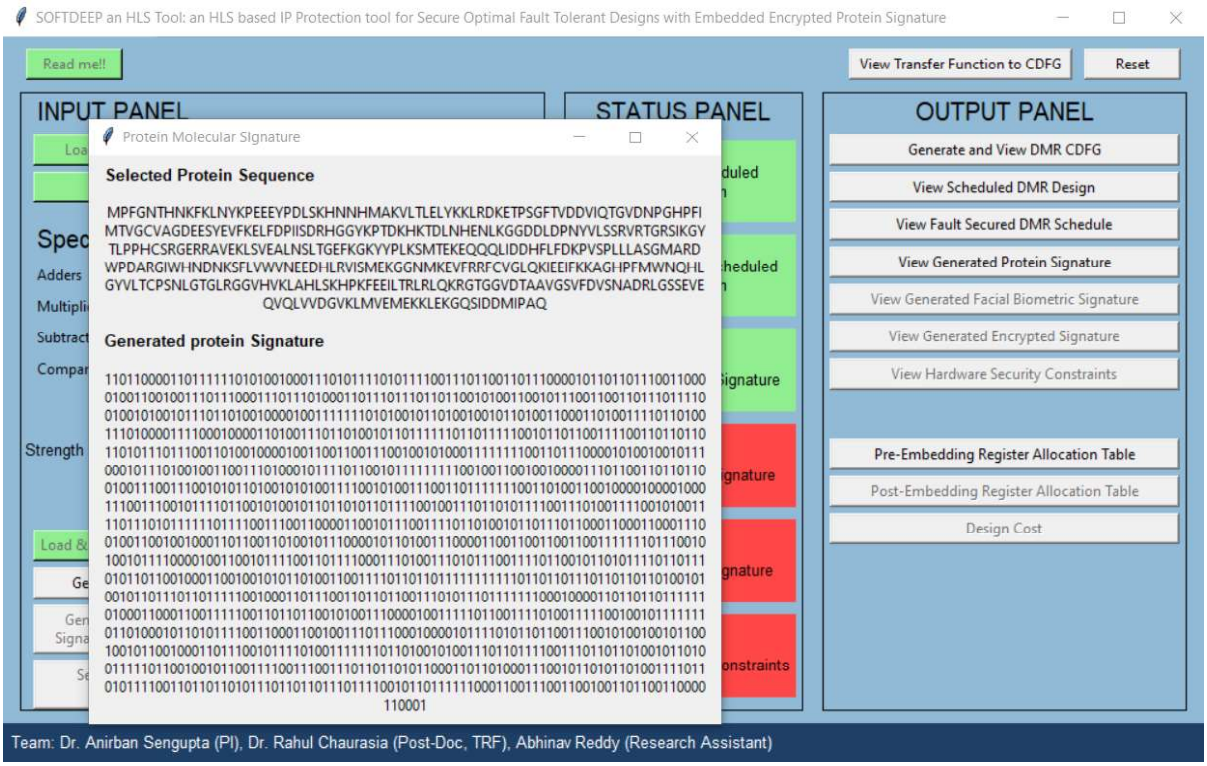


→Post selecting IP vendor's protein molecular sequence, its corresponding signature gets generated and the tab 'View generated Protein Signature' in the output panel gets enabled and the Tab 'Generating Protein Molecular Signature' turns GREEN in the status panel, as shown below:

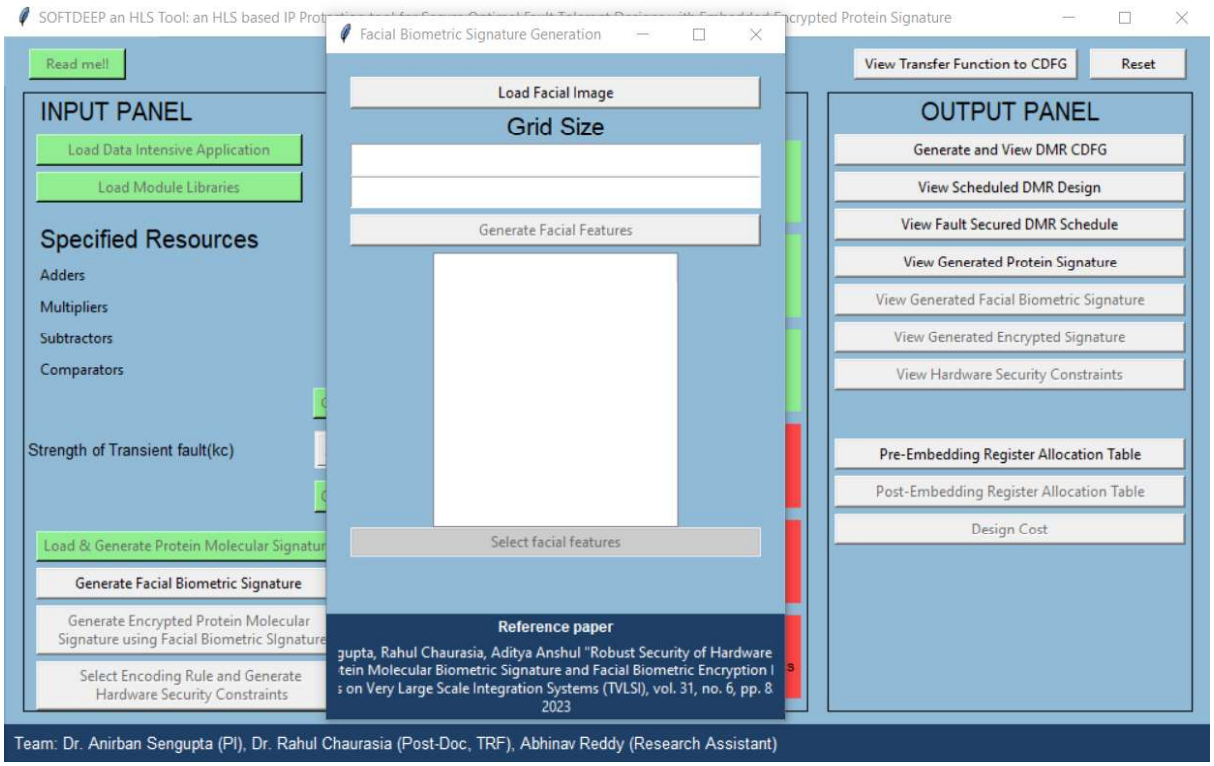


This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

→Now, user can view generated protein signature by clicking on its Tab. The output screen is shown below

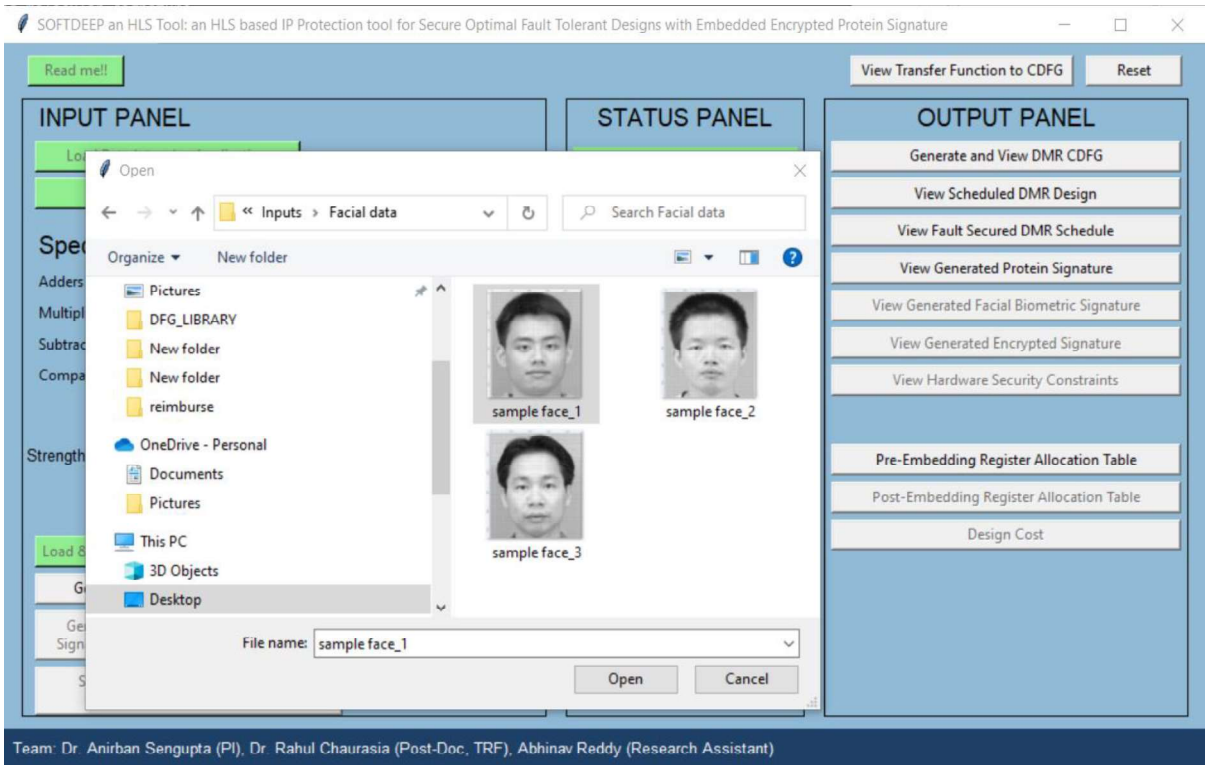


STEP-7: Next, the user is asked to generate facial biometric signature corresponding to captured facial biometrics image of IP vendor/user. By clicking the Tab 'Generate Facial Biometric Signature' a pop-up window appears for the user (to perform following tasks such as 'Load Facial Image' and select 'Grid Size' to generate image with facial features for generating facial biometric signature based on selected facial features) as shown below.

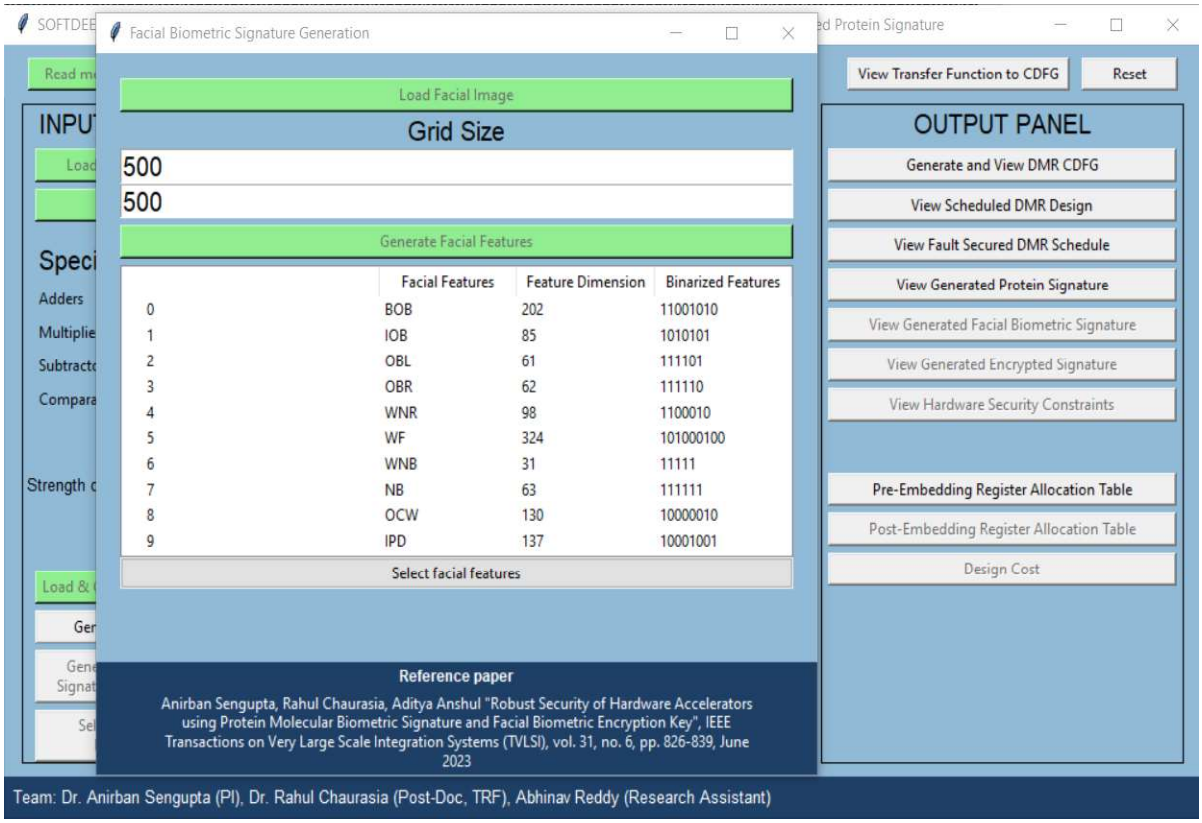


This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

→By clicking on Tab 'Load Facial Image' a pop-up window appears for the user to select facial image as shown below:

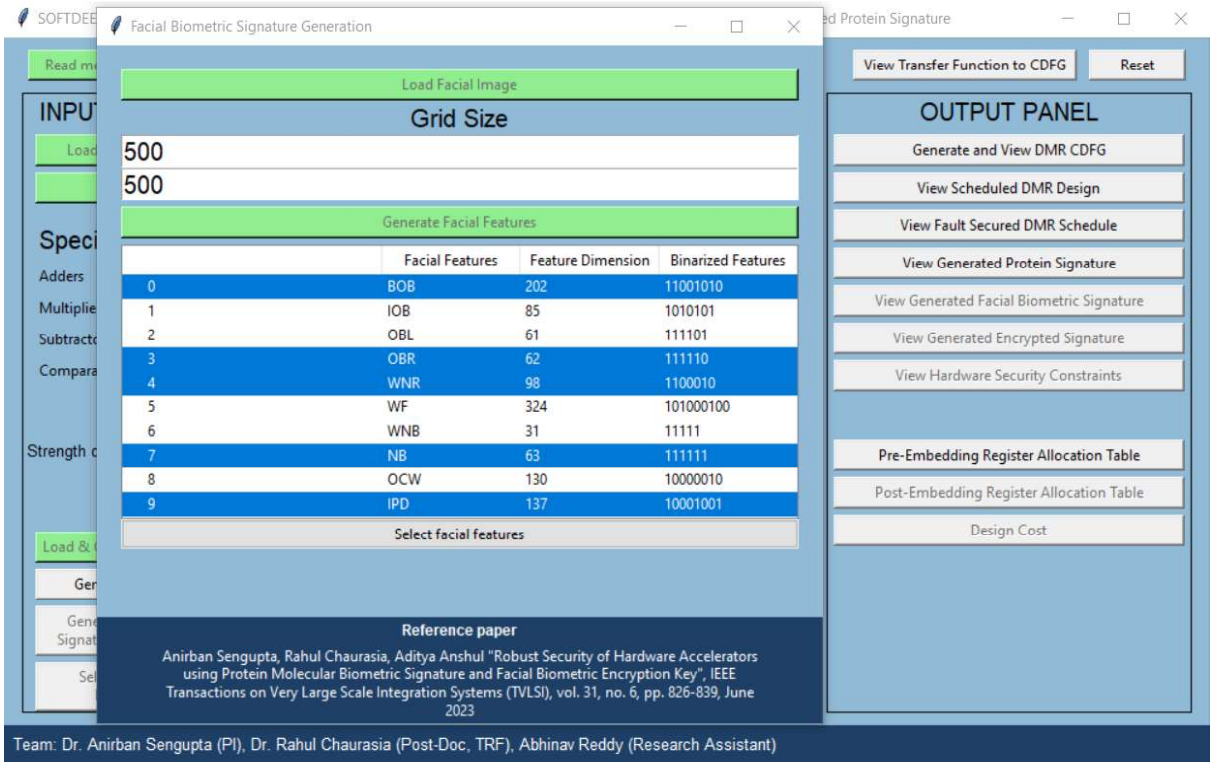


→Post loading the facial image, Tab 'Load Facial Image' turns GREEN as shown below. Next the user enters grid size (e.g., 500X500). Next by clicking Tab 'Generate Facial Features' facial features, features dimensions and their corresponding binarized signature is generated and it turns GREEN and as shown below:

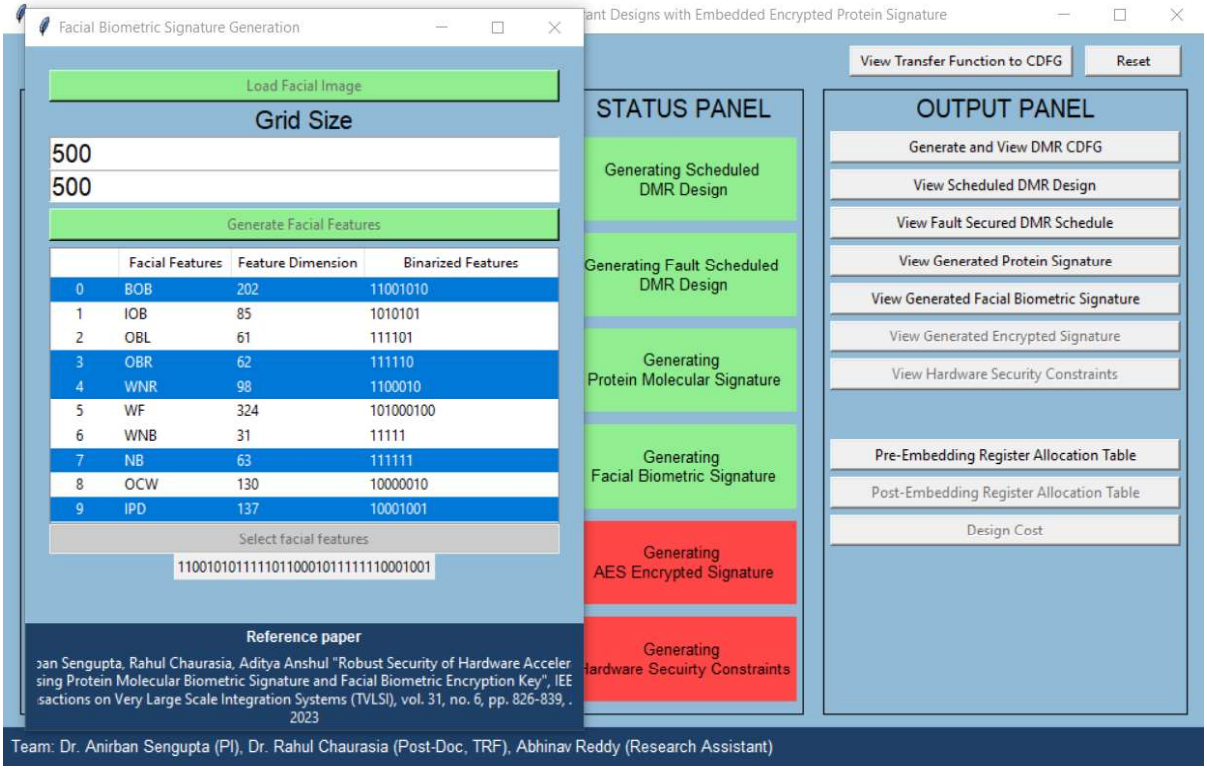


This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

→Next, IP vendor/user is facilitated to select facial features (amongst the generated features) for generating the final facial signature post concatenation. *Note: the features in BLUE indicates the IP vendor/user selected features*.

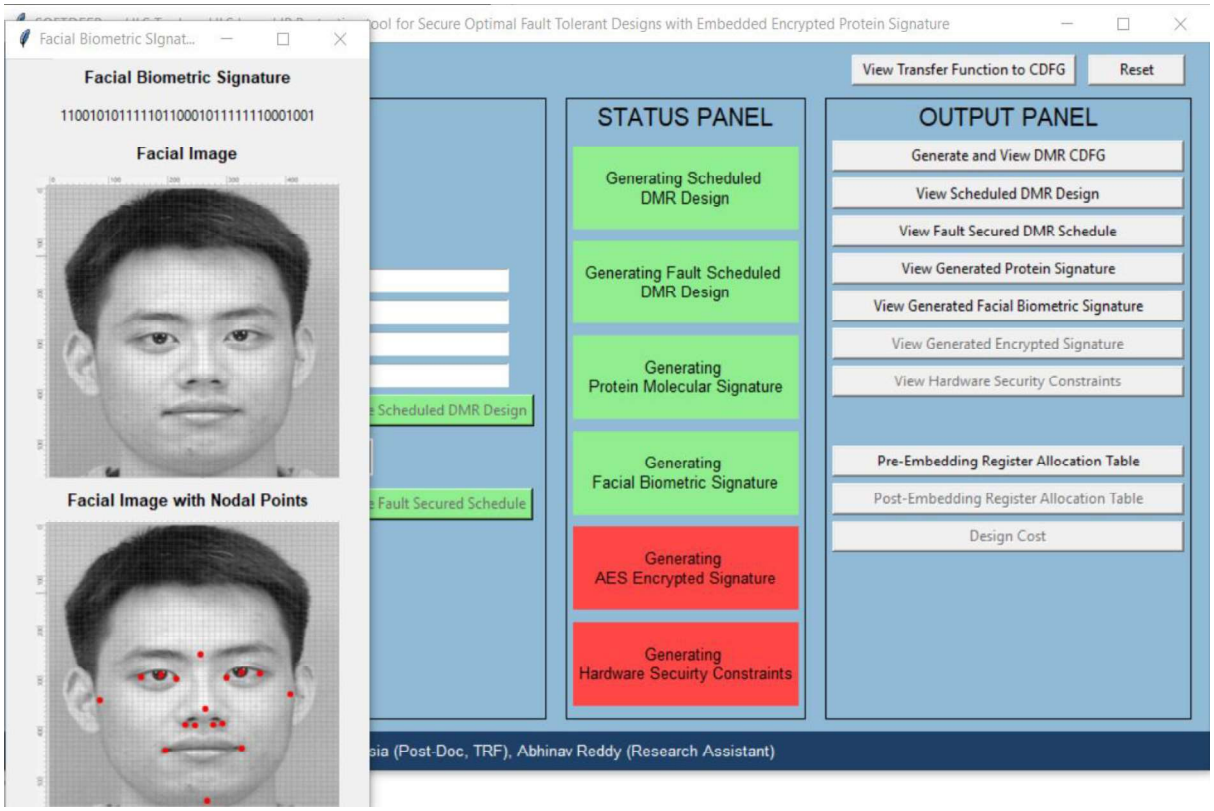


→Next, by clicking on the Tab 'Select facial features' final facial signature is generated (to be used as encryption key in 'AES' framework) and the Tab 'Generate encrypted Protein Molecular Signature using Facial Biometric Signature' in the input panel and the Tab 'View Generated Facial Biometric Signature' in the output panel gets enabled and the Tab 'Generating Facial Biometric Signature' turns GREEN in the status panel as shown below:

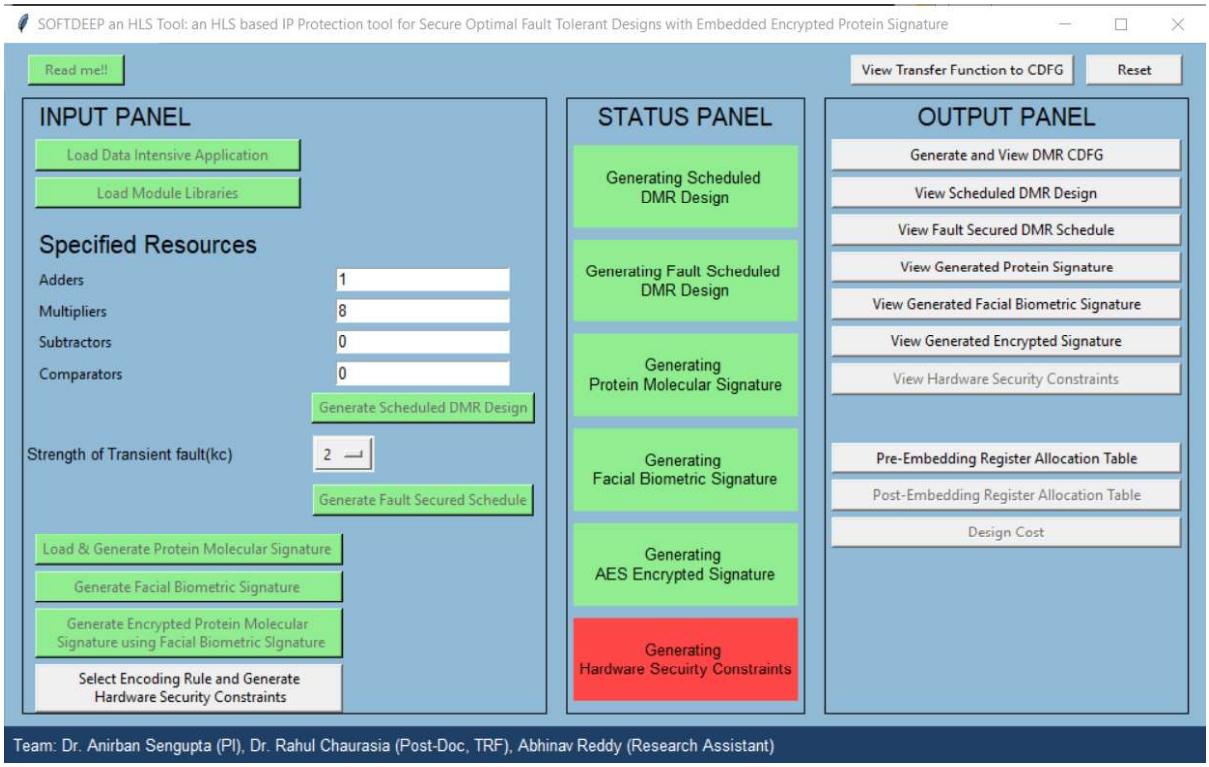


This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

→Now, user can view the facial image with facial features corresponding to captured facial image and generated facial biometric signature. The output screen is shown below:

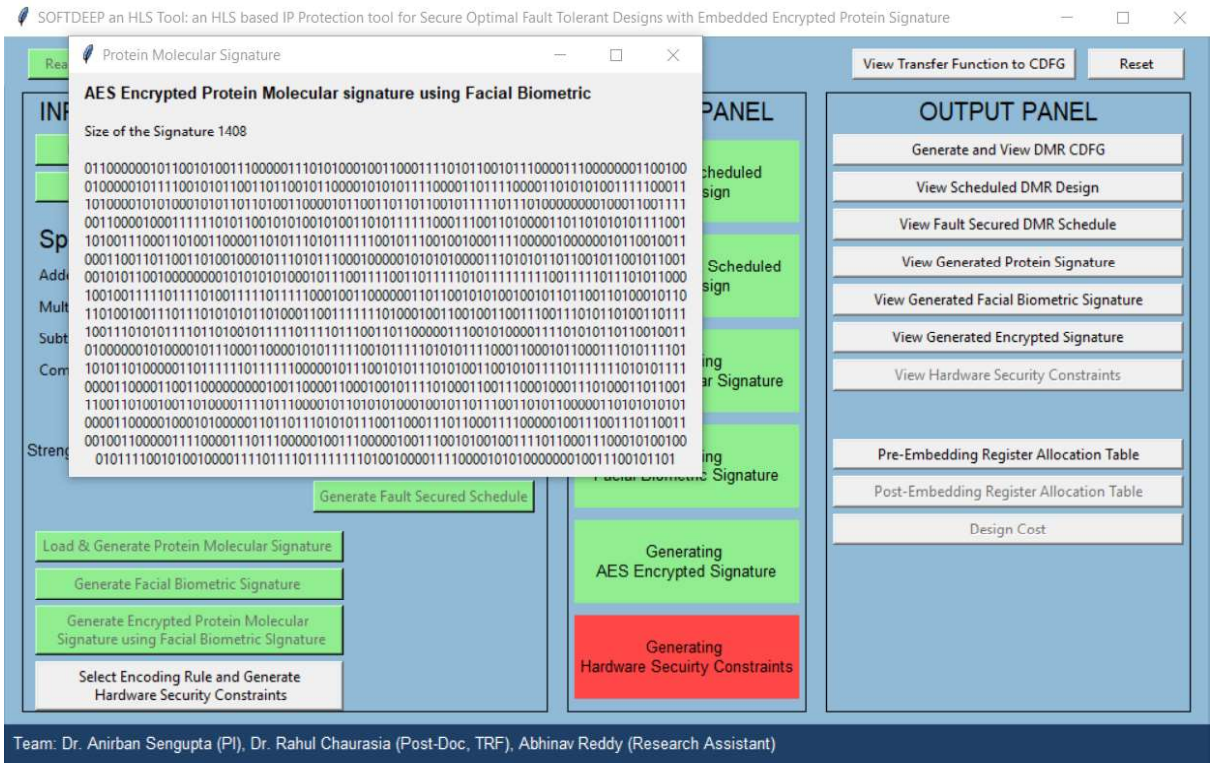


STEP-8: Next, user can generate encrypted protein molecular signature by using facial biometric signature as encryption key. By clicking on Tab 'Generate Encrypted Protein Molecular Signature using Facial Biometric Signature' a Tab 'Select Encoding Rule and Generate Hardware Security Constraints' in the input panel and the Tab 'View Generated Encrypted Signature' in output panel gets enabled and Tab 'Generating AES Encrypted Signature' in the status panel turns GREEN as shown below:

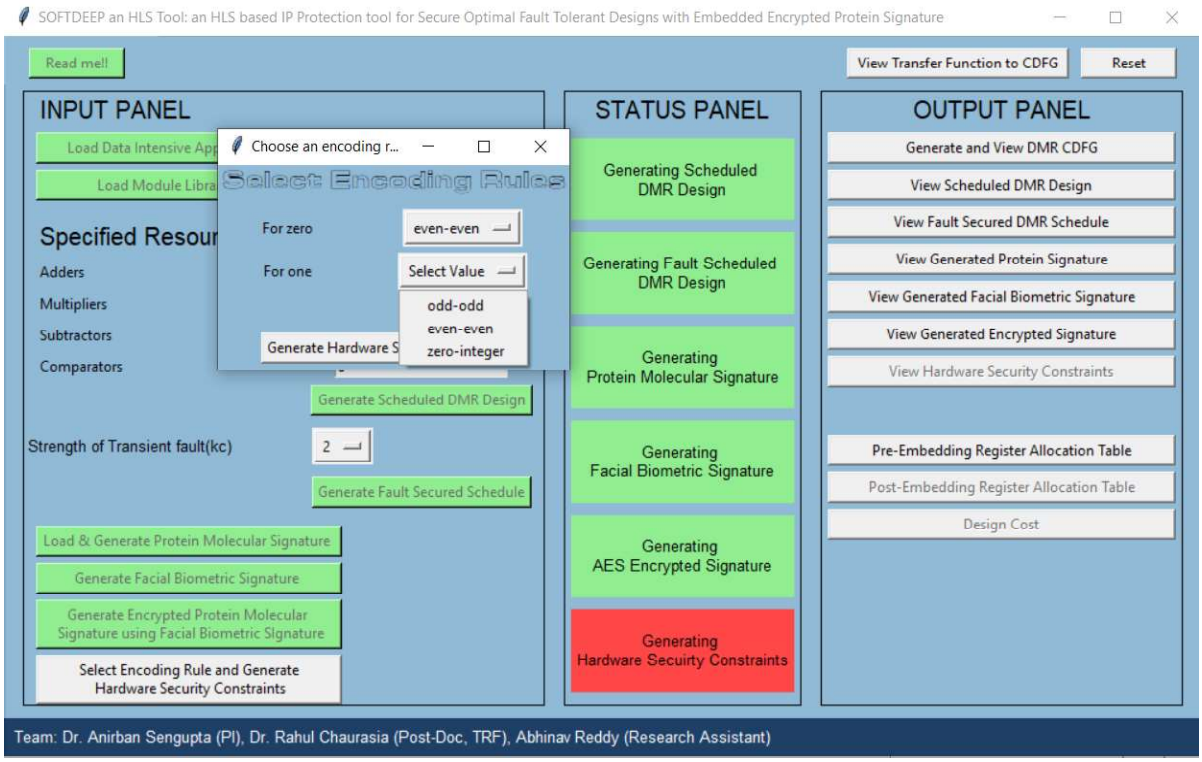


This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

→User can view the generated encrypted signature by clicking on Tab 'View Generated Encrypted Signature' as shown below:

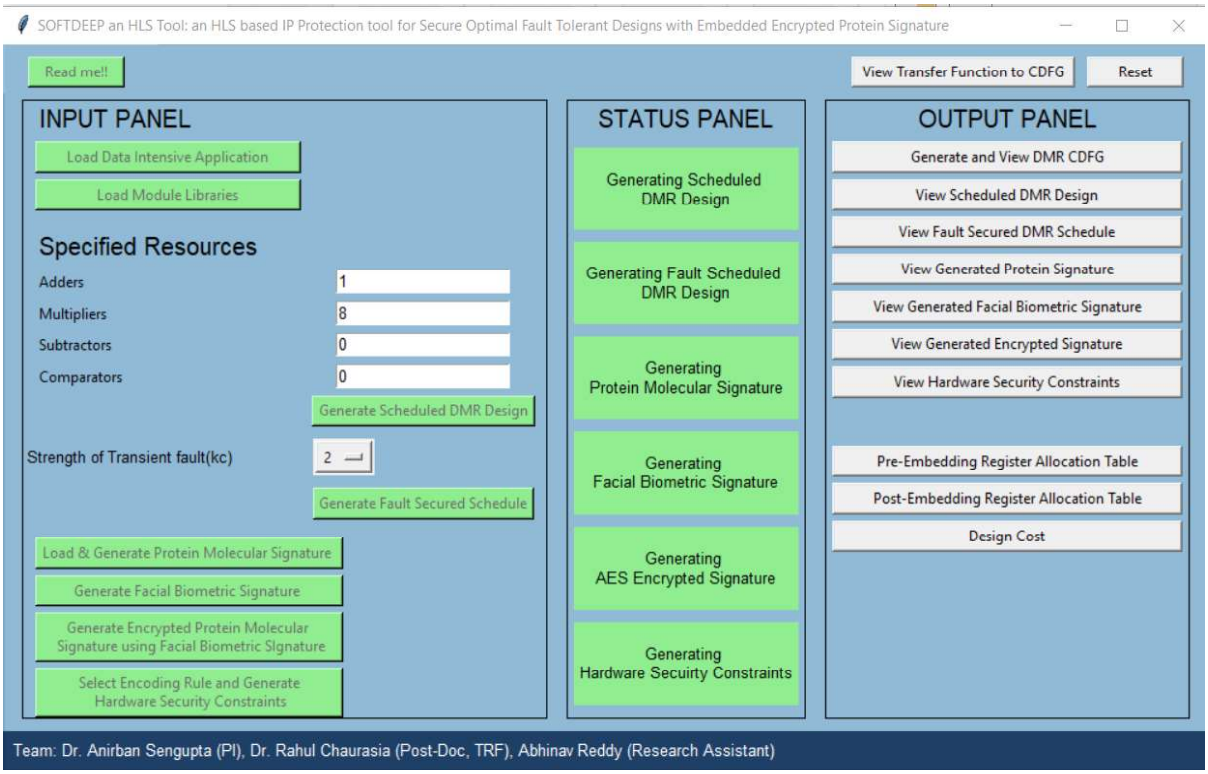


STEP-9: Next, user can generate hardware security constraints corresponding to encrypted signature using encoding rule by clicking on Tab' Select Encoding Rule and Generate Hardware Security Constraints'. Post clicking on Tab a pop-up window appears for user to select encoding rules. User can select any of the available encoding rules from the dictionary (for generating covert hardware security constraints) as shown below:

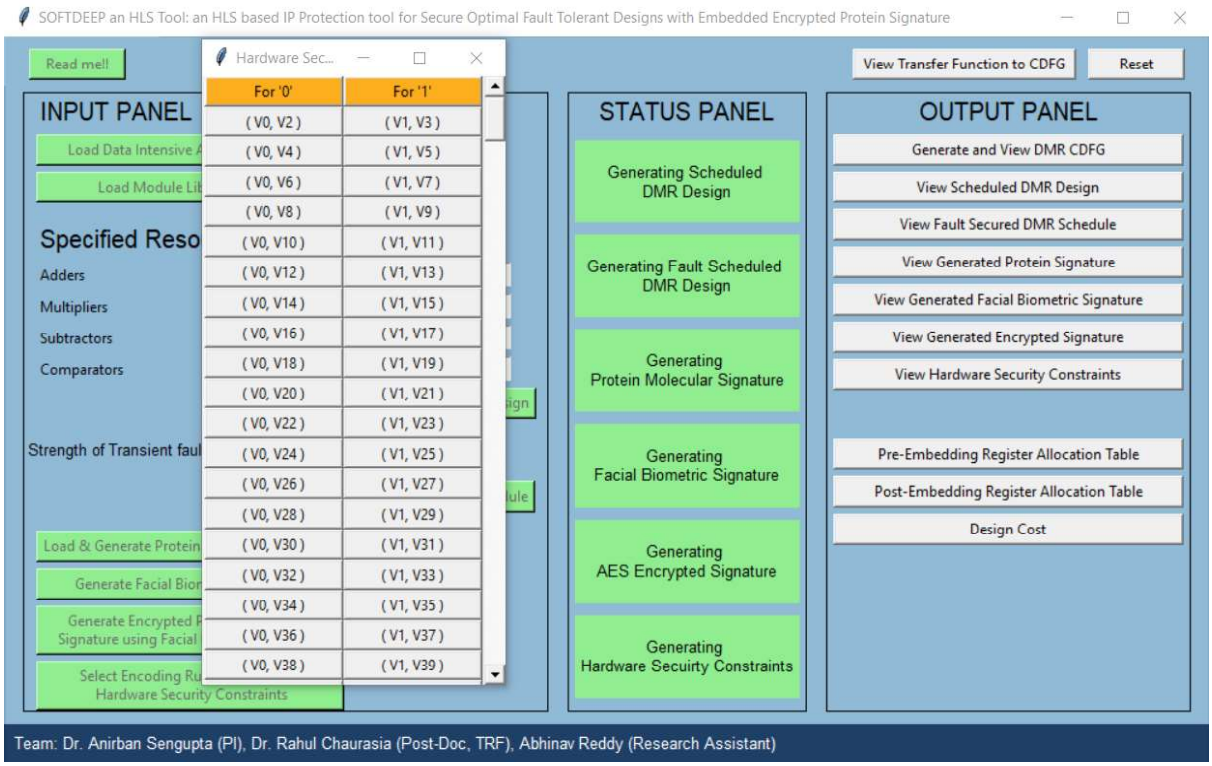


This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

→Next, by clicking on Tab 'Generate Hardware Security Constraints' in pop-up window, Tabs 'View Hardware Security Constraints', 'Post-Embedding Register Allocation Table' and 'Design Cost' in the output panel gets enabled and the Tab 'Select Encoding Rule and Generate Hardware Security Constraints' in the input panel and the Tab 'Generating Hardware Security Constraints' in the status panel turns GREEN as shown below:

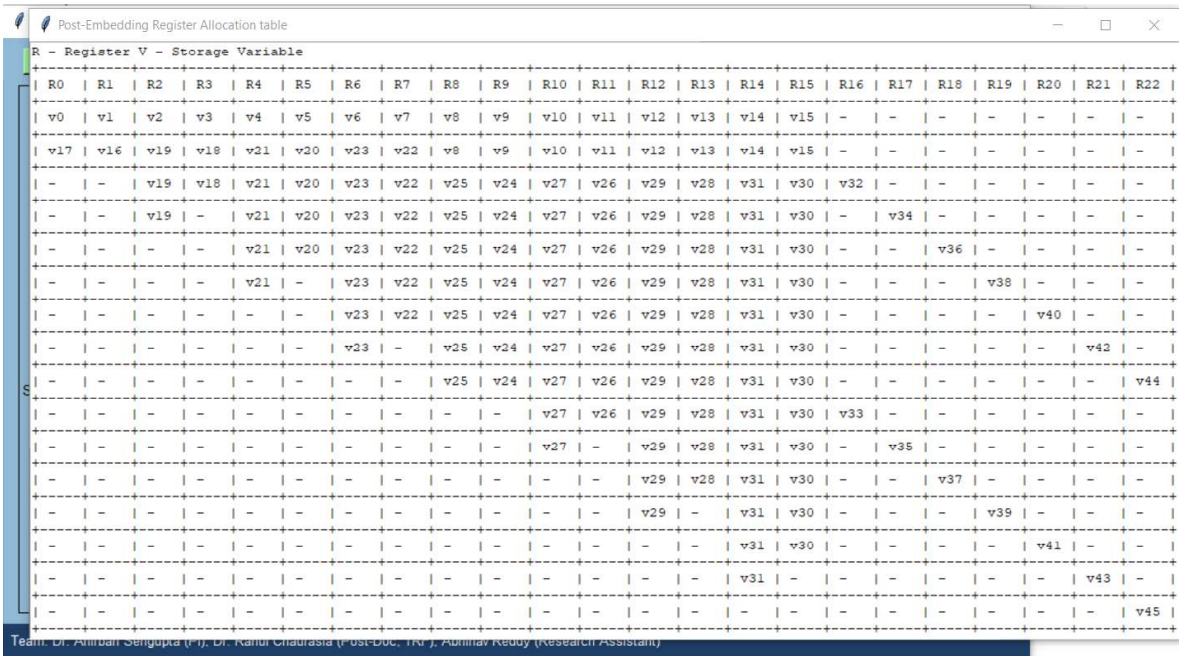


→User can view the generated hardware security constraints by clicking on the Tab 'View Hardware Security Constraints'. The output screen is shown below:

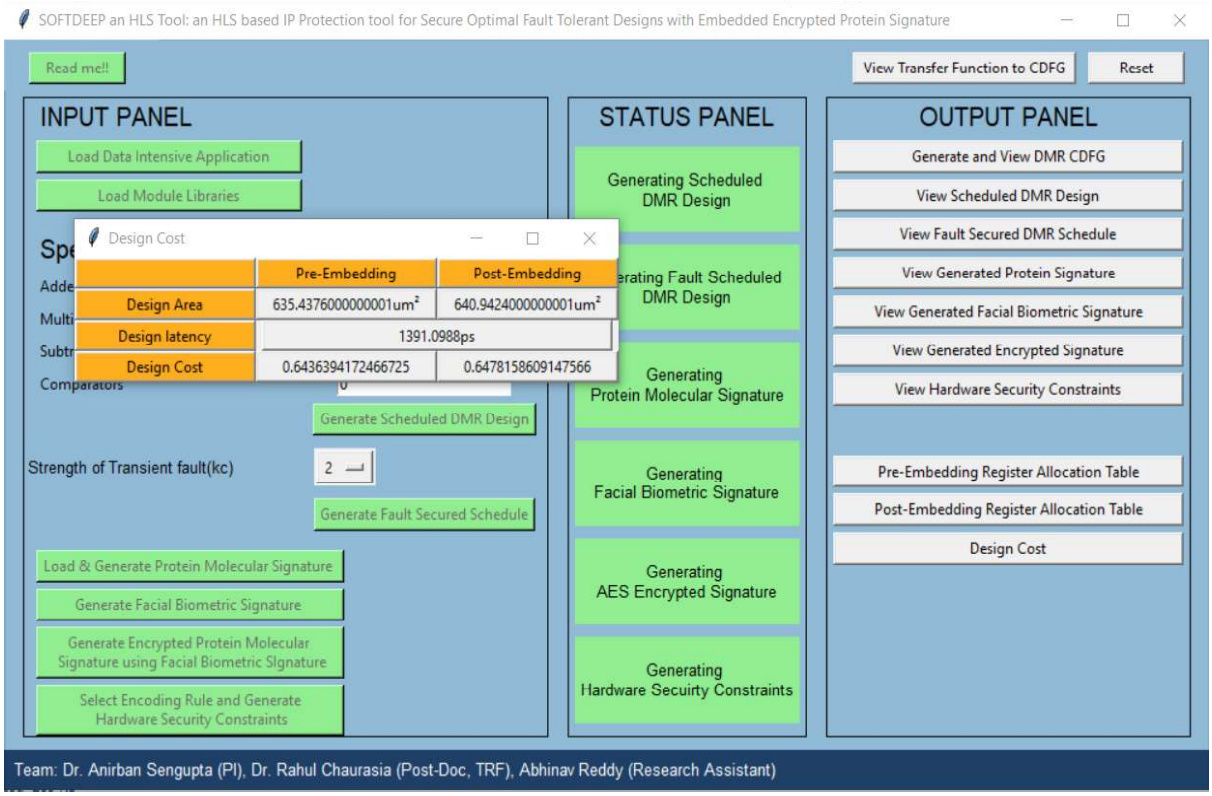


This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

→User can view post-embedding register allocation table by clicking on the Tab 'Post-Embedding Register Allocation Table'. The output screen is shown below:

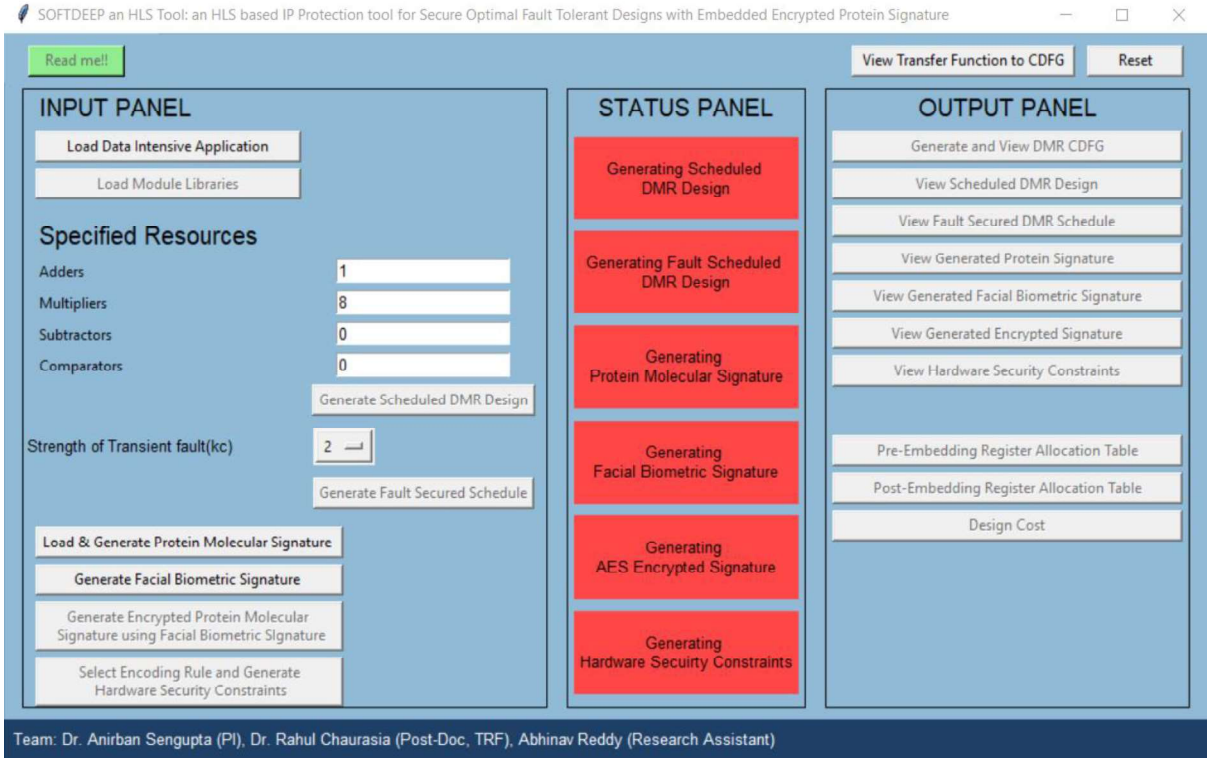


→Further, user can view design cost for generating the secure optimal K-cycle fault tolerant data path processor for input application with embedded encrypted protein molecular biometric by clicking on the Tab 'Design Cost'. Thus, the secure optimal K-cycle fault tolerant data path processor design for input application with embedded encrypted protein molecular biometric as piracy detective countermeasure is generated during HLS. The output screen is shown below:

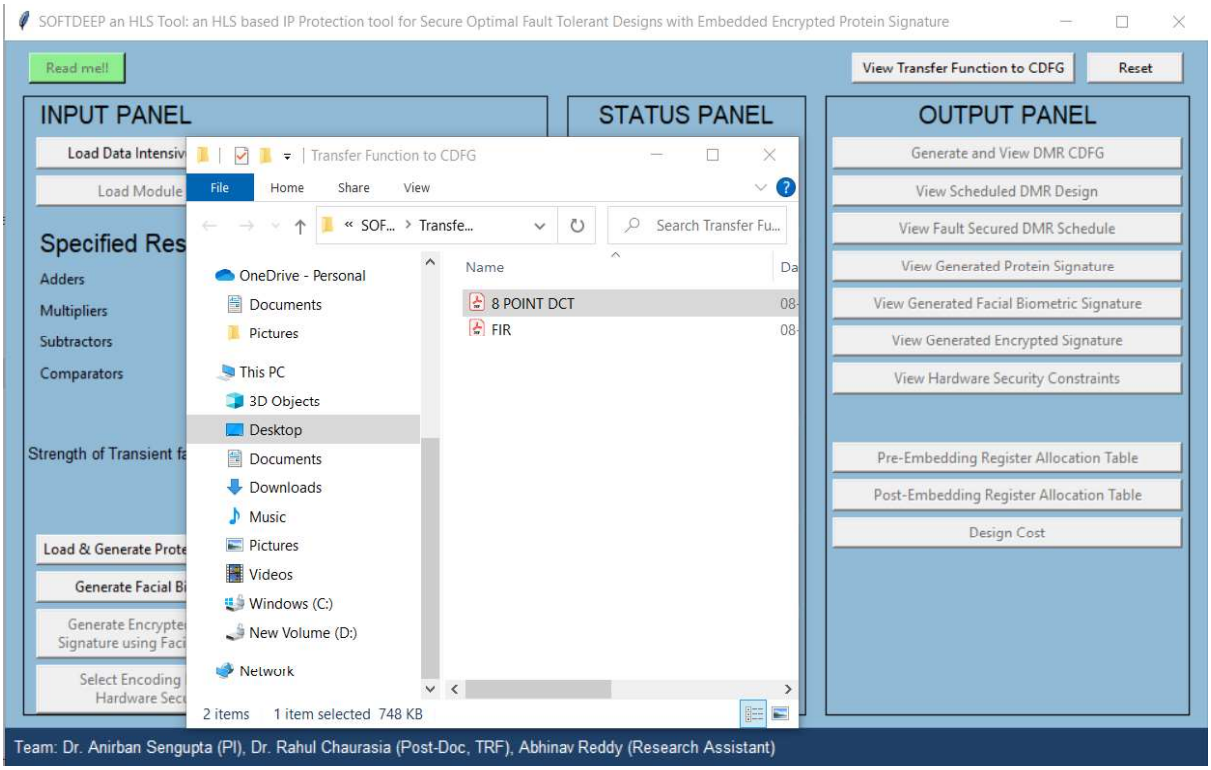


This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)

STEP-10: RESET: By clicking on the Tab 'Reset', user can reset the provided details for configuring the data path processor design (secure and optimal K-cycle fault tolerant design with detective control against piracy) based on chosen different hardware resources, strength of transient fault (Kc), protein molecular sequence of varying sample and strength and facial biometrics information, either for the same application or any other data intensive applications. The output screen post clicking on the Tab 'Reset' is shown below:



Note: By clicking on the Tab 'View Transfer Function to CDFG' user can also view the details of deriving the CDFG of the sample application from their transfer function. The output screen is shown below:



This tool has been developed under the supervision of Dr. Anirban Sengupta (PI and Supervisor) and Dr. Rahul Chaurasia Post-Doc (TRF)