IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 9, Issue 4, Aug - Sep 2021
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Reduction Of Effect Of Multiple Hardware Trojans In Crypto processor

P. **Ramesh , K. Bhanu, B. Nikitha, K. Pretham**
Students, ALIET , Vijayawada
Andhra Loyola Institute of Engineering and Technology
Vijayawada, Andhra Pradesh, India.

***Abstract*— Outsourcing IC design and fabrication is one of the effective solution to reduce the design cost but it may cause severe security risks. A hardware trojan is a form of malicious circuitry that damages the function or and trustworthiness of an electronic system. The payload of an hardware trojan is the entire activity that the trojan executes when it is triggered. Malicious trojans try to bypass or disable security fence of a system .It is important to provide security against hardware trojan attacks in electronic systems. Thus, by providing security against these attacks the confidential information can't be accessed by hackers.With the help of our proposed model, we can detect and prevent multiple hardware trojans.**

Keywords — Hardware Trojan , Cryptography, IC security, Blowfish Encryption Algorithm , Character Encryption

Introduction

As the Electronic age increases and expands every day the production of IC's becomes more and more important and essential to keep up the electronic race. The increasing production of IC leads to vulnerable attacks on them by so-called attackers or adversaries. As an IC is utilized by most of the firms the attacks on ICs result as a great threat to, financial Organizations, military systems, transportation systems, and household appliances as well. The Attacks of a Hardware Trojan appear always to be a great threat for widely electronics but majorly pointing towards the integrated circuits (ICs). Causing a non-observable modification internally in an IC and resulting in leaking of information to untrustworthy people and manipulating data while still lurking in the design without even getting noticed by anyone. The Attacker or the one who inserts the trojan makes it stealthy which does not get noticed in post-manufacturing tests but activates during field operation. As the number of trojans gets increased its payloads differ concerning their trigger points. It is not necessary that every Trojan inside a single design must provide the same loss or damage. Every other Trojan has its own way to unleash damage on the design. Some Trojans can affect at the output port by manipulating the provided data as input. Some Trojans can leak the most confidential information to the adversaries. But the Trojans that work on manipulating the input data are the most faced ones. From the very old times to this new extending era facing a hardware Trojan can be a mind boggling task. Even the ones who are called as adversaries doesn't know about the Trojan the are about to place but they can control the threshold point which triggers the activation of Trojan. That threshold point can be a particular voltage, a particular amount of data or a particular set of data. Irrespective of the reason a hardware Trojan still creating problems in every electronic device we can name, many techniques are still developed and used. But there is none technique which shares a spotlight or a golden prevention method which can be used on any Trojan occurred on any device. Still the journey to detect and prevent a hardware Trojan has a long path to take and long miles to go.

Detection Methods

Physical Inspection

In this Methodology, the upper layer is sliced to uncover the hardware. Then, the architect examines more than once the surface to pounding the layers of the chip. Including this, there are other techniques to examine the hardware. Most strategies are:Light-Induced Voltage Alteration (LIVA),Scanning electron microscopy (SEM), Pico-second imaging circuit analysis (PICA), Scanning optical microscopy (SOM), Voltage Contrast Imaging (VCI), Charge Induced Voltage Alteration (CIVA). To understand the basic design of the chip, a photograph of the chip is taken and even contrasted. To distinguish Trojan equipment that incorporates (crypto) keys that are extraordinary, a picture difference can be taken to uncover the distinctive design on the chip. The lone known equipment Trojan utilizing special crypto keys however having a similar design is. This property upgrades the imperceptibility of the Trojan.[3]

Functional Testing:

During this method, the designs' output is taken into consideration for determining any fabrication issues. If the yielded output is not the same as the expected output, then there a presence of a hardware trojan. But this method is not helpful all the time as the output can defer because of internal design issue rather than the effect of a trojan found. [1] [4]

Built-in Self Test:

Built-in Self Test (BIST) and Design For Test (DFT) procedures add hardware (rationale) to the chip planned to help check that the chip, as constructed, executes its practical determination. The additional rationale screens input upgrade and interior signs or memory states, by and large by figuring checksums or by uncovering inward registers through an altered filtering procedure. Where DFT normally facilitates with some outside testing component, BIST-enabled chips join custom test-design

generators. BIST usefulness frequently exists to perform at-speed (high velocity) check where it's anything but conceivable to utilize filter chains or other low-speed DFT capacities. The two strategies were initially evolved to distinguish fabricating mistakes, yet additionally have the twofold edged potential to recognize a few impacts of vindictive rationale on the chip, or to be abused by noxious rationale to secretly assess far off state inside the chip.[4]

Side-Channel Analysis:

Each device that is electrically dynamic discharges various signs like attractive and electric fields. Those signs, that are brought about by the electric movement, can be examined to acquire data about the state and the information which the gadget measures. Progressed strategies to quantify these results have been created and they are touchy (side-channel assault). Henceforth, it is feasible to identify firmly coupled Trojans by means of estimation of these simple signs. The deliberate qualities can be utilized as a mark for the dissected gadget. It is additionally not unexpected that a bunch of estimated values is assessed to keep away from estimation mistakes or different errors.[5]

Prevention methods

Given the extensive dangers presented by the presence of Hardware Trojans, one approach to guarantee they can't influence a plan is by keeping them from being embedded at any stage of the IC advancement cycle. Counteraction is the primary opportunity to counter the danger of Hardware Trojans. It's anything but a crucial connection in a guard top to the bottom system. There are generally the typical approaches, procedures, and best rehearses that can be utilized to keep up authority over the IC advancement measure: using confided in people, plan devices, and confided in manufacture offices as effectively portrayed. Some particular exploration portraying novel strategies for forestalling Hardware Trojans at various phases of the IC improvement life-cycle has been finished. This exploration has taken a gander at counteraction during the plan, manufacture, and post-creation phases of an IC. Prevention is the essential chance to counter the peril of Hardware Trojans. It's anything but's an essential interface in a protection method to framework. There are by and large the average methodologies, strategies, and best practices that can be used to keep up power over the IC headway measure: utilizing trusted in individuals, plan gadgets, and trusted in produce workplaces as adequately depicted. Some specific investigation depicting novel systems for preventing Hardware Trojans at different periods of the IC improvement life-cycle has been done. This investigation has looked at countering during the arrangement, production, and post-creation periods of an IC. There are different techniques for trojan prevention but we will look into some of the major ones.

Prevention by Design:

This strategy exploits the perception that while it very well might be hard to totally determine a plan so all assets are completely used, it is generally easy to check whether a given plan fulfills this prerequisite. Thus, the creator proposes utilizing untrusted, business CAD apparatuses to make the plan, and a little, self-assembled (hence trusted) device to watch that a given plan does in fact fulfill the prerequisites. The essential issue with this methodology is that it is completely conceivable to fabricate a Hardware Trojan predominantly from the rationale that as of now exists in a plan. While it could be moderately easy to foster an instrument to watch that a given plan utilizes all accessible equipment assets, guaranteeing that there are no noxious impacts of that plan would appear to be a more troublesome recommendation.[6] [7]

Prevention by Fabrication:

It is a methodology whereby a portion of the IC's plan is carried out by reconfigurable rationale (to be indicated post creation) is portrayed by Baumgarten, Tyagi and Zambreno (2010). Reconfigurable rationale is put between the yields of certain IC's and the contributions of different ICs, camouflaging a portion of the plan from an aggressor who approaches the RTL. This methodology might be viewed as either a precaution measure or a strategy for working within the sight of Hardware Trojans; as such it is additionally nitty-gritty in Section 6.3. As far as its preventive ascribes, it's anything but an aggressor unsure of the specific operations of the IC until after the reconfigurable rationale has been customized. This chops down the aggressor's open door. Indeed, even given best endeavours it is hard to totally forestall the expansion of Hardware Trojan rationale to ICs. All that that can be accomplished is an initial phase in a blend of steps to counter the presence of Hardware Trojans.[8]

Encryption:

we can perform encryption on data during the trojan activation by comparing the original data with the trojan-affected data. We can do this by keeping an alternate path as a reference path to compare and even hide the alternate path from system design.[1] The output of the comparator gives a status signal for the intimation of Trojan detection and drives the control input of the switching circuit. The changes of main path data are observed, the comparator generates a negative signal to the switch control for data change. The switch circuit terminates main path signals and connects parallel path signals to cipher, so the original results are achieved even though Trojan is activated.[10]

blowfish crypto processor

Blowfish is symmetric encryption algorithm,that means it uses same key to both encrypt and decrypt the data.The blowfish algorithm is also known as block cipher. The flow diagram of blowfish is shown in fig1 below. In these algorithm it divides the message in to fixed length blocks while performing encryption and decryption.The block length of the blowfish is 64 bits.The graphical representation of this algorithm is shown below.Generally a blowfish algorithm is a replacement of DES,IDEA algorithm. In these the size of plain text is 64-bits & the size of key is varies from 32 to 448 bits that means in blowfish cipher key size is not fixed. If we are not mentioning anything by default it will take the key size is 128-bits and it performs 16 rounds. In this algorithm the original key is divided into different number of sub keys .Generally this are divided into 18 sub-keys .Let us name it as p1,p2,p3……p18. These all sub-keys are called as P-arrays. Along with division of sub-keys our original key is also divided into different number of S-boxes. In DES and IDEA algorithm ,we have S-boxes but in DES algorithm the S-box

does not depend on key. S-boxes are individual structure. But in blowfish algorithm we are deriving S-boxes of size 32-bit from the original key. At each S-box contains approximately 256 entries. In these first ,we initialize P-array and S-box with some null values, after p1 is XOR' ed with first 32-bit of the key and second 32-bit XOR' ed with p2 and so on up to p18. In this algorithm it divides the plain text into two equal half's. For suppose assume as a left and Right part. After dividing perform XOR operation on the left part with p1 of P-array. g result. Now this result is applied to a function 'F'.After applying a function we are getting some output that output is XOR' ed with right part. After performing this operation the result which we got is moved to left part and the result which we got after performing XOR between the left part and p1 in previous ,that result is moved to right part and repeat the same procedure for 16 number of times. That means at the 16th round we re performing XOR between the p16 and the result from the right part in 15th round. After completion of 16th round we do not make any swapping operation.Apply P17 and p18 to each part individually. That means apply p17 to right part and p18 to left part.

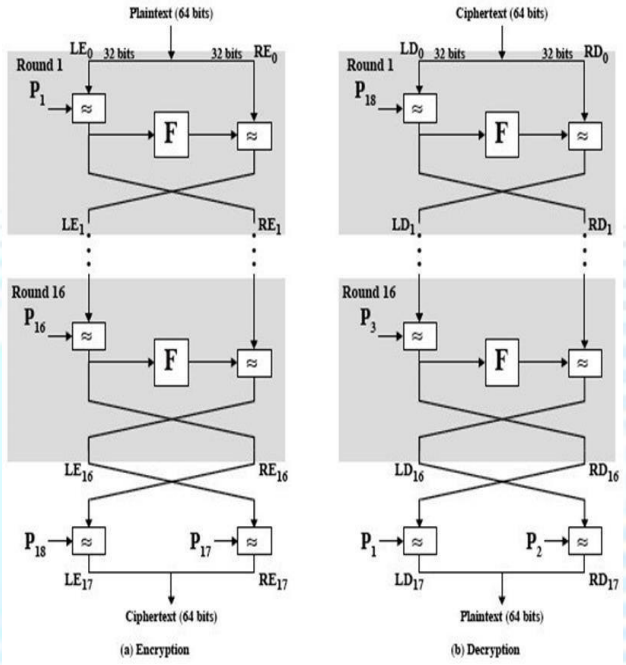


Fig.1. Flow diagram of Blowfish Crypto Processor

a) Encryption b) Decryption

Character encryption

A Hardware Trojan always trigger on a rare event, which can even be a particular data. If we can change that rare event, we can deactivate them. Hence we secure and encrypt that particular data that triggers the trojan.Our proposed model is using Character Jumbling to perform transposition on the data so that the rare event is not a rare event any more.Procedure for performing Character Jumbling is first by performing a Data Reversal and then Data Rotation.

Fig.2. **(a)** Input after Data Reversal

From the above fig , when the input "electronics" is passed as input we get reversed output as "scinortcele".

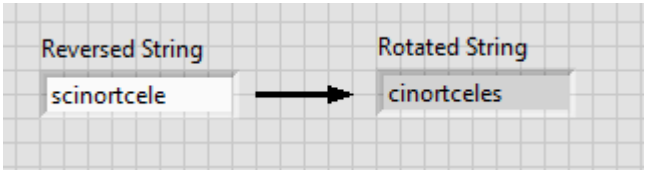


Fig.2. **(b)** Reversed input after Data Rotation.

From the above fig , when the reversed input "scinortcele" is passed as input, we get the rotated output as "cinortceles".Which is the final output from Character Encryption block. Hence by using the data reversal operation followed by data rotation operation, we can jumble the data even without the effort of using a separate transposition algorithm which increases the complexity of the design.

proposed model

In the proposed model, a secured system for detecting and preventing multiple trojans are discussed and implemented, The block diagram for multiple trojan detection is given fig2 below,

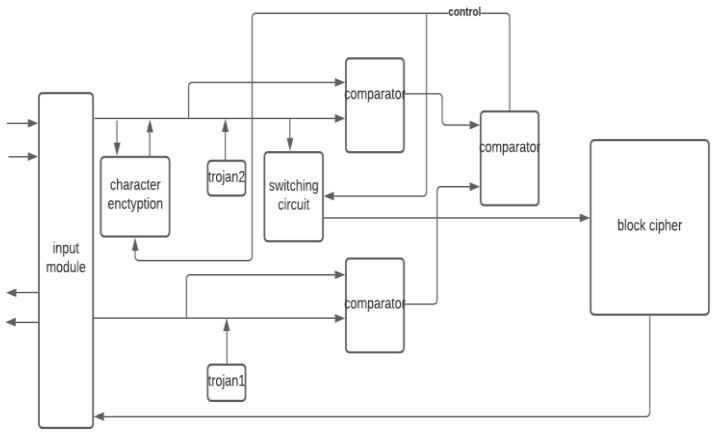


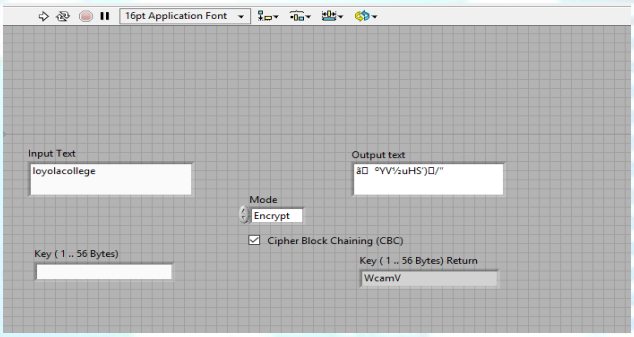
Fig.3. Block Diagram of Multiple Trojan detection and correction in cryptoprocessor.

Working:

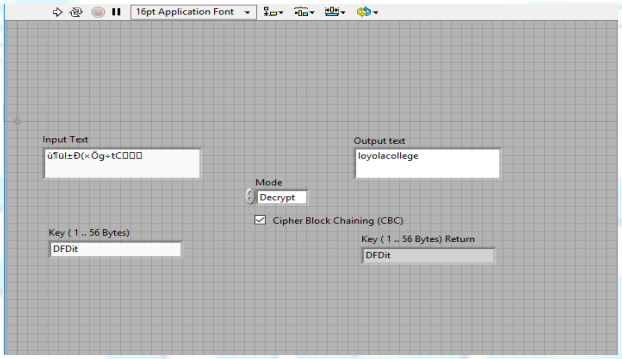
The proposed model is dealing with the multiple trojans. For this model we are having two paths one is main path & other one is alternate path . Our proposed Model deals on the condition that both the paths have trojans since a trojan is placed on free area . Initially the two trojans are in deactivation state. when we send the data through the input module, the data is travel along the both paths. Each of the paths contain a comparator making them the main comparators and a secondary comparator is present for further validation. Initially, the input data we are sending through the path is duplicated and provided as one of the input for the comparator, and the other input is the data though the path. Both the comparators pass data only when equality condition is satisfied (i.e) When both the inputs for the comparator are same, else it would close the path that doesn't satisfy this condition.This happens when both trojans are deactivated and if either one of them are activated. Up until now the main comparators do their job and secondary comparator is in off state. When both the trojans are activated both comparator outputs are compared and then the secondary comparator turns ON and then passes the control to character encryption block. From now onwards all the input data moves through the character encryption block and jumbles the data to make the rare event not so rare any more hence by deactivating the trojan the data is passed to the receiver.

Results:

In this section we present simulation results of our proposed method as set of LabVIEW front panel pictures. In this we compared the results of Trojan free circuit, Trojan effected circuit and our proposed . ALL the results for our proposed model are as follows,



(a)



(b)

Fig.4. Results of Trojan free output using Blowfish Algorithm **(a)**Encryption **(b)**Decryption

In **fig 4.a** when the text "loyolacollege" is applied as input for the encryption block, we got the ciphered text and in **fig 3.b** when the ciphered text is decrypted we got the original text message. This is the trojan free output. As we are working on multiple trojans, **fig3** should be similar to all trojans initially.

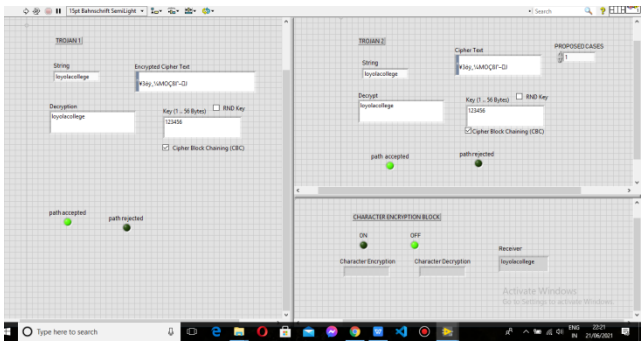


Fig.5. Case 1 where Trojan1 and Trojan2 are in deactivation state(T1=0,T2=0)

In **fig5** When the text "loyolacollege" is passed as input, cipher text was obtained and after decryption, we got the original text message on both the paths which means that both the trojans are in deactivation state and the input message is passed to the receiver.

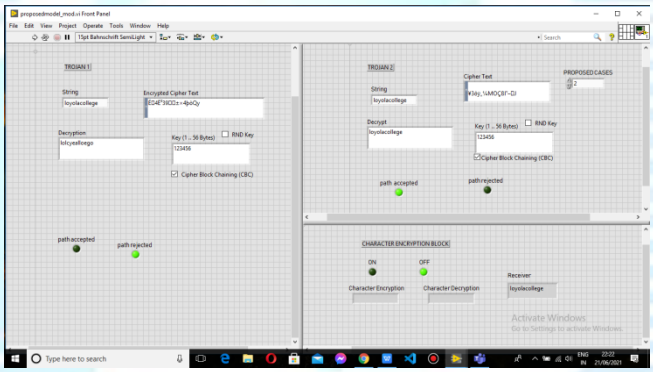


Fig6. Case 2 where Trojan1 is activated and Trojan2 is in deactivation state(T1=1,T2=0)

In **fig6** When the text "loyolacollege" is passed as input, cipher text was obtained and after decryption, we got the wrong text on the main path and original text in the alternate path which means that trojan1 on main path is activated and trojan 2 on the alternate path is still in a deactivation state. Now the input text passes through the alternate path since main path is blocked due to trojan activation.

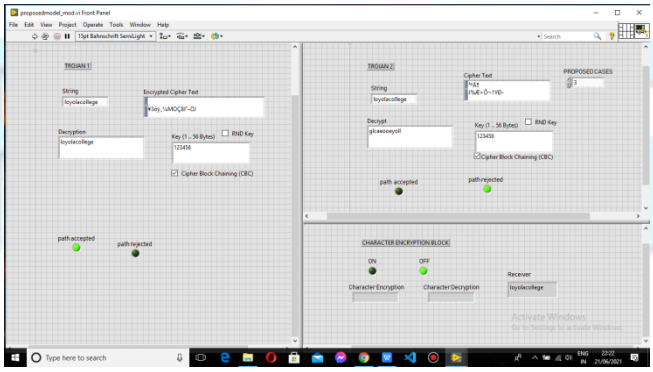


Fig7. Case 3 where Trojan1 is deactivated and Trojan2 is in activation state(T1=0,T2=1)

In **fig7** When the text "loyolacollege" is passed as input, cipher text was obtained and after decryption, we got the wrong text on the alternate path and original text in the main path which means that trojan1 on main path is in deactivation state and trojan 2 on the alternate path is activated . Now the input text passes through the main path since alternate path is blocked due to trojan activation

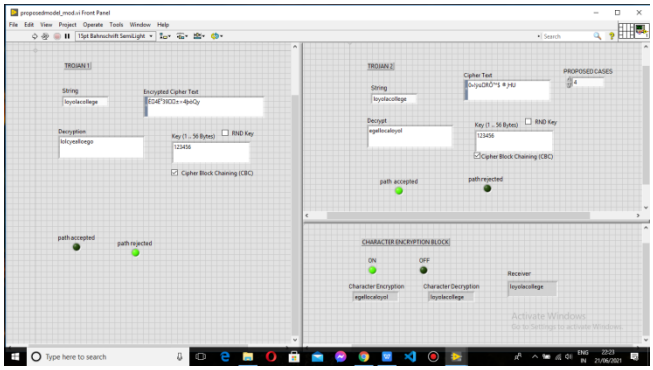


Fig8. Case 4 where Both Trojan1 and Trojan2 are in activation state (T1=1,T2=1)

In **fig8** When the text "loyolacollege" is passed as input, cipher text was obtained and after decryption, we get the wrong input on both the paths since both trojans are activated. Now the character encryption block gets activated and jumbles the input data so that the trojan goes into deactivation state and passes the data through the path to the receiver. Generally speaking handling can be a tedious task but from Our Proposed Model we can detect and correct multiple hardware trojans in a cryptoprocessor.

Table 1: Working Status

Proposed Cases	Description
00	Both the trojans are in deactivation state.
01	Trojan 2 affects the data
10	Trojan 1 affects the data
11	Character encryption block jumbles the data to deactivate one of the trojan.

Conclusion.

Handling a trojan can be a tedious task in any period of time. There are several papers for detection and prevention methods regarding the effect given by a single hardware trojan. But by using our proposed model we can detect and prevent the effect of multiple trojans lurking in the same circuit as well. In this paper, we proposed a method for detecting and preventing the effect of multiple hardware trojans using Blowfish Encryption Algorithm and Character Encryption with the help of labView simulation tool.

Acknowledge

The authors of this paper would like to thank Department of Electronics and Communication Engineering and Management of Andhra Loyola Institute of Engineering and Technology for their valuable suggestions and support.

References

[1] "Reduction Of Hardware Trojan Effect Using. Multipath Authentication". P.Bosebabu, K. Siva Nagaraju, B. Chanikya, P. Ritish Kumar www.ijstr.org.

[2] "Advancing the State-of-the-Art in Hardware Trojans Detection".IEEE Transactions on Dependable and Secure Computing, Vol 16,N0 1, January/February 2019 Syed Kamran Haider, Chenglu Jin, Masab Ahmad, Devu Manikantan Shila, Omer Khan and Marten van Dijk,

[3] "A survey on hardware trojan detection techniques". Bhasin, S., & Regazzoni, F. (2015). 2015 IEEE International Symposium on Circuits and Systems (ISCAS). doi:10.1109/iscas.2015.7169073

[4] " Test generation for combinational hardware Trojans" Wang, Sying-Jyan & Wei, Jhih-Yu & Huang, Shih-Heng & Li, Katherine Shu-Min. (2016). . 1-6. 10.1109/AsianHOST.2016.7835569.

[5] "A survey of hardware Trojan threat and defense,Integration" He Li, Qiang Liu, Jiliang Zhang, Volume 55, 2016.

[6] Beaumont, Mark & Hopkins, Bradley & Newby, Tristan. (2021). Hardware Trojans – Prevention, Detection, Countermeasures (A Literature Review).

[7] HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Chakraborty, R. S., & Bhunia, S. (2009). 28(10), 1493–1502. doi:10.1109/tcad.2009.2028166.

[8] Baumgarten, A., Tyagi, A., & Zambreno, J. (2010). Preventing IC Piracy Using Reconfigurable Logic Barriers. IEEE Design & Test of Computers, 27(1), 66–75. doi:10.1109/mdt.2010.24

[9] "Design and implementation of a private and public key crypto processor and its application to a security system". IEEE Transactions on Consumer Electronics, 2014 Ho Won Kim, and Sunggu Lee,

i