How Can Blockchain Technology Help Improve User Security and Privacy?

Building Blockchain based Cryptosystems: A Case Study

Security Privacy and Trust in Group Key Agreements using Blockchain Smart Contract Centric Computing

Introduction

- In modern world, most of the wireless systems require ***resource constrained*** devices such as RFID tags, sensors, smart cards, small processors, PDA's, and smart phones.

- These *devices* play a major role in providing security for ***satellite communication, internet security, e-banking, e-commerce, Internet of Things (IOT) applications, and embedded systems***.

- Implementing ***security for a wireless communication system*** using these devices is the most challenging problem.

- Many cryptographic algorithms were developed to accomplish their ***requirements*** for secure data communication in ***wireless systems.***
- These algorithms have many limitations, which include ***increased power consumption, communication, and computational*** complexity with increased processing time.
- Thus, an ***efficient cryptographic*** algorithm that ***overcomes*** these ***limitations*** is the need of the hour.

Secure Group Communication

- With the exponential growth in modern communication, ***secure group communication*** (SGC) is becoming an important research area
- In various ***group ware applications***, such as teleconferencing, tele-medicine, real-time information services, distributive interactive simulations, grid computing, and collaborative work.
- This communication refers to a group of participants that helps in ***sending and receiving messages to/from other group members*** in a way that outsiders are unable to make any information even when they can intercept the messages.

DLP-based Protocols

- Most of the ***group key agreement*** protocols are ***DLP***-based.
- However, the key length for secure ***DLP-based D–H*** has increased over recent years, which has also placed a ***heavier processing*** load on applications
- Making them not suitable for the ad-hoc network's due to ***limited bandwidth, slower CPU speed, limited battery power,*** and have high bit-error rate wireless links.

Problems with Current State of Art

- Conventionally, numerous single node burdened group key algorithms based on D-H were proposed.
- These prior art methods mainly aim on networks in which a few member's acts as power-embarrassed devices.
- This system expects to be with n nodes and n – 1 member executes a couple of exponentiations to get the key, while one member implements n exponentiations.
- The node n faces more burdens comparing to other nodes, due to computing and communicating particular value to every node.
- In light of its chosen secret and using the value from node n, every node can figure the group Key.

Problems with Current State of Art

- Conventionally, numerous single node burdened group key algorithms based on D-H were proposed.
- These prior art methods mainly aim on networks in which a few member's acts as power-embarrassed devices.
- This system expects to be with n nodes and n – 1 member executes a couple of exponentiations to get the key, while one member implements n exponentiations.
- The node n faces more burdens comparing to other nodes, due to computing and communicating particular value to every node.
- In light of its chosen secret and using the value from node n, every node can figure the group Key.

Problems with Current State of Art

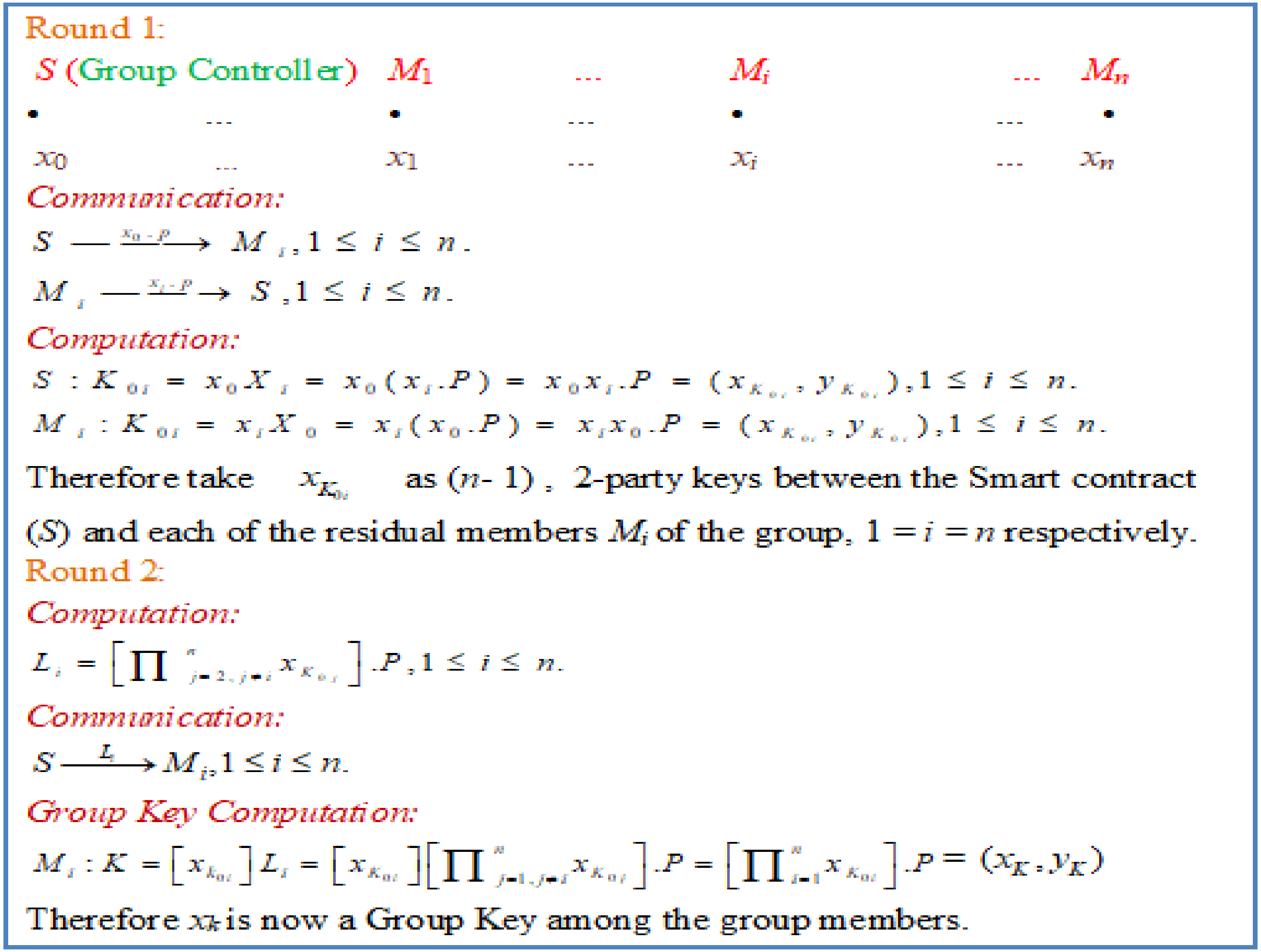
The recent group key agreement entails:

- lightweight computing
- reduced communication,
- decentralized certification,
- personal privacy protection such as traceability and accountability, etc.
- There is a need for an enhanced blockchain decentralized processing technology which helps in reducing the computation and communication burden of each member.

Problem Statement

- Therefore, there is a need for a system that addresses ***one node burdened*** centric dynamic group key agreement protocols.
- A blockchain technology is needed that allows group members to exchange data without involving ***the third party*** for the establishment of trust.
- There is a need for a system that is light weight and easily *adaptable to large wireless ad-hoc networks* with an equal ***constant minimal processing time on every node***.
- There is a need for an enhanced system that helps in ***diminishing the computation and communication burden*** of each member and providing an anonymous identity authentication to protect personal privacy.
- There is a need for a smart contract that ***detects and tracks the malicious attempts*** that disrupts the generation of a group key among the members.

Base Group Key Agreement



Round 1:

S (Group Controller) M_1 ... M_i ... M_n

• ... • ... • ... •

x_0 ... x_1 ... x_i ... x_n

Communication:

$S \xrightarrow{x_0 \cdot P} M_i, 1 \leq i \leq n.$

$M_i \xrightarrow{x_i \cdot P} S, 1 \leq i \leq n.$

Computation:

$S : K_{0i} = x_0 X_i = x_0(x_i.P) = x_0 x_i.P = (x_{K_{0i}}, y_{K_{0i}}), 1 \leq i \leq n.$

$M_i : K_{0i} = x_i X_0 = x_i(x_0.P) = x_i x_0.P = (x_{K_{0i}}, y_{K_{0i}}), 1 \leq i \leq n.$

Therefore take $x_{K_{0i}}$ as $(n- 1)$, 2-party keys between the Smart contract (S) and each of the residual members M_i of the group, $1 = i = n$ respectively.

Round 2:

Computation:

$L_i = \left[\prod_{j=2, j\neq i}^{n} x_{K_{0j}}\right].P, 1 \leq i \leq n.$

Communication:

$S \xrightarrow{L_i} M_i, 1 \leq i \leq n.$

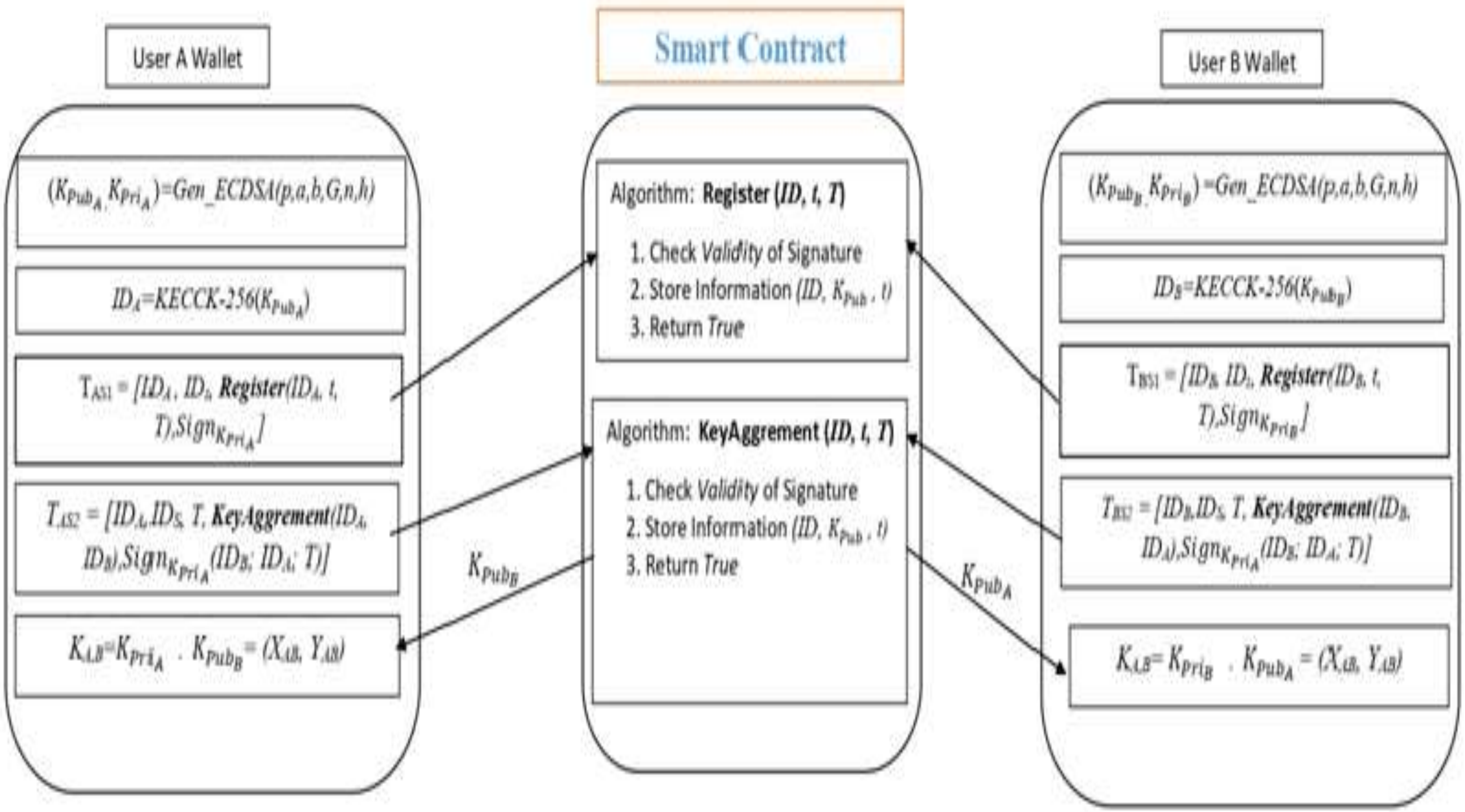
Group Key Computation:

$M_i : K = \left[x_{k_{0i}}\right] L_i = \left[x_{K_{0i}}\right]\left[\prod_{j=1, j\neq i}^{n} x_{K_{0j}}\right].P = \left[\prod_{i=1}^{n} x_{K_{0i}}\right].P = (x_K, y_K)$

Therefore x_k is now a Group Key among the group members.

ACGKA Protocol

Blockchain processing for two party key agreement



User A Wallet

(K_{Pub_A}, K_{Pri_A})=Gen_ECDSA(p,a,b,G,n,h)

ID_A=KECCK-256(K_{Pub_A})

T_{AS1} = [ID_A, ID_S, **Register**(ID_A, t, T),$Sign_{K_{Pri_A}}$]

T_{AS2} = [ID_A,ID_S, T, **KeyAggrement**(ID_A, ID_B),$Sign_{K_{Pri_A}}$(ID_B; ID_A; T)]

K_{AB}=K_{Pri_A} . K_{Pub_B}= (X_{AB}, Y_{AB})

Smart Contract

Algorithm: **Register (*ID, t, T*)**

1. Check *Validity* of Signature
2. Store Information *(ID, K_{Pub} , t)*
3. Return *True*

Algorithm: **KeyAggrement (*ID, t, T*)**

1. Check *Validity* of Signature
2. Store Information *(ID, K_{Pub} , t)*
3. Return *True*

K_{Pub_B}

K_{Pub_A}

User B Wallet

(K_{Pub_B}, K_{Pri_B}) =Gen_ECDSA(p,a,b,G,n,h)

ID_B=KECCK-256(K_{Pub_B})

T_{BS1} = [ID_B, ID_S, **Register**(ID_B, t, T),$Sign_{K_{Pri_B}}$]

T_{BS2} = [ID_B,ID_S, T, **KeyAggrement**(ID_B, ID_A),$Sign_{K_{Pri_A}}$(ID_B; ID_A; T)]

K_{AB}= K_{Pri_B} . K_{Pub_A} = (X_{AB}, Y_{AB})

Blockchain Based Three Party Key Agreement

Let *A*, *B* and *C* are three parties wants to establish a *GK* among them.

Round1:

- All the Group users should register in Blockchain network.
- After registration each group member should establish a two party key with Smart contract *(S)* using Blockchain two-party shared key agreement.
- Let the shared keys of *A*, *B*, *C* with *S* be K_{SA}, K_{SB} and K_{SC} respectively.

Round2:

- If *A*, *B*, and *C* wants to set up a GK among them each of them have to initiate a transaction which includes all the ID's of group members and invoke the Smart contract.
- Now this Smart contract validates the group members and transaction if its valid.
- Smart contract first compute product of all two party shared keys produced in round 1 as $Prod = K_{SA} * K_{SB} * K_{SC,}$ and Hides it from others.

- Further, producing partial group key using the computed product and inverse of the respective participants shared key.
- After receiving the partial group key sent by Smart contract, each of the group member generates the group key by multiplying the received product with its shared key .
- Now all the group participants established the *GK* as

$K_{SABC} = K_{SA} * K_{SB} * K_{SC}$

Blockchain based Dynamic Group Key Agreement:

Join Protocol

1. If a registered participant*D* wants to join into already established group of *S*, *A*, *B* and C. It first generates a two party key with Smart contract namely K_{SD}.
2. Now this *S* generates a random number called R_D and then it sends $R_D * K_{SD}$to all the three group participants.
3. Now This *S* sends $R_D * K_{SABC}$ to the member *D*.

4. Now the group members *A*, *B*, *C* computes the new *GK* as follows

$K_{SABCD} = R_D * K_{SD} * K_{SABC}$

5. The group member *D* computes group key by as follows

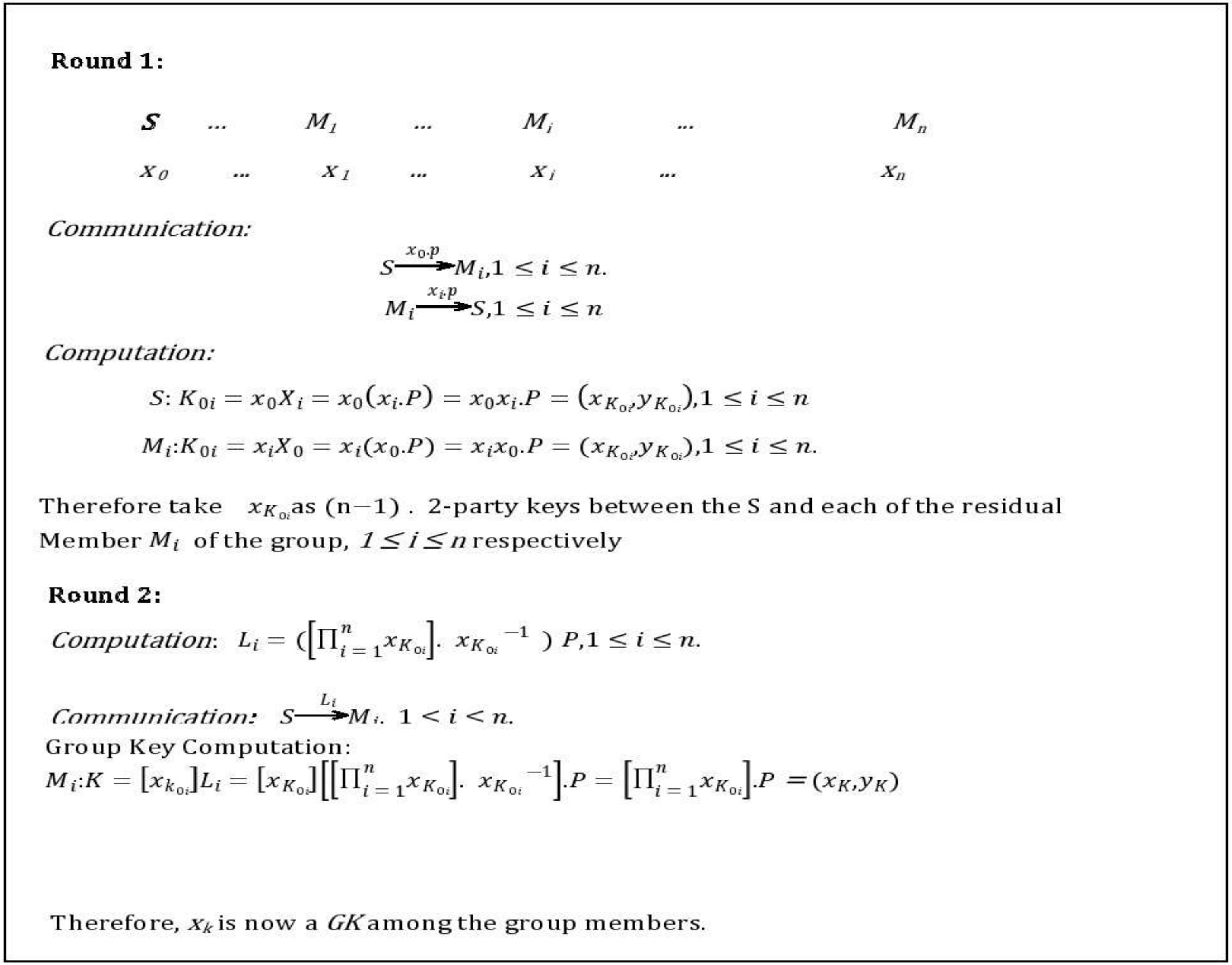
$K_{SABCD} = R_D * K_{SABC} * K_{SD}$

Leave Protocol:

1. If a registeredparticipant*B* desires to Leave the group from *S*, *A*, *B*, *C*. Now *B* has to inform to the *S* by invoking Leaving method.
2. Now Smart Contract generates a random number called R_B and then it sends $R_B * K_{SB}^{-1}$ to all the remaining group participants.
3. Now each of the group member computes the updated key as follows

$K_{SAC} = R_B * * K_{SABC}$

B-ACGKA Protocol



Round 1:

S	...	M_1	...	M_i	...	M_n
x_0	...	x_1	...	x_i	...	x_n

Communication:

$$S \xrightarrow{x_0.p} M_i, 1 \le i \le n.$$

$$M_i \xrightarrow{x_i.p} S, 1 \le i \le n$$

Computation:

$$S: K_{0i} = x_0 X_i = x_0(x_i.P) = x_0 x_i.P = (x_{K_{0i}}, y_{K_{0i}}), 1 \le i \le n$$

$$M_i: K_{0i} = x_i X_0 = x_i(x_0.P) = x_i x_0.P = (x_{K_{0i}}, y_{K_{0i}}), 1 \le i \le n.$$

Therefore take $x_{K_{0i}}$ as (n−1) . 2-party keys between the S and each of the residual Member M_i of the group, $1 \le i \le n$ respectively

Round 2:

Computation: $L_i = \left(\left[\prod_{i=1}^{n} x_{K_{0i}}\right].\ x_{K_{0i}}{}^{-1}\right) P, 1 \le i \le n.$

Communication: $S \xrightarrow{L_i} M_i.\ 1 < i < n.$

Group Key Computation:

$$M_i: K = [x_{k_{0i}}]L_i = [x_{K_{0i}}]\left[\left[\prod_{i=1}^{n} x_{K_{0i}}\right].\ x_{K_{0i}}{}^{-1}\right].P = \left[\prod_{i=1}^{n} x_{K_{0i}}\right].P = (x_K, y_K)$$

Therefore, x_k is now a *GK* among the group members.

Dynamic Join Protocol

i) Once a fresh participant M_{n+1} needs to join the group, it notifies the Smart Contract and produce a two party-ECDH key $x_{K_{0,n+1}}$ with S.

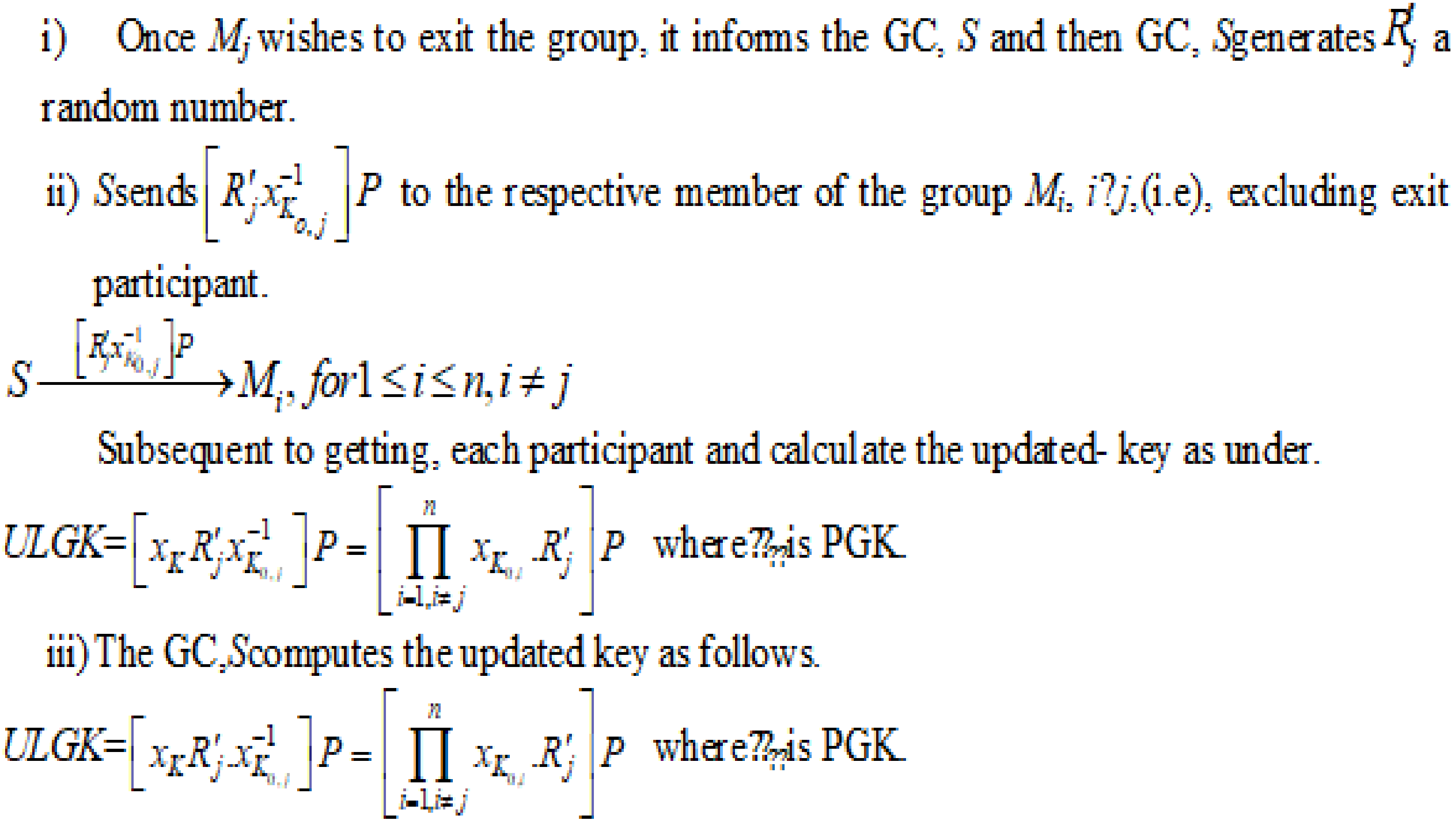
ii) The$S$Produces R'_{n+1} aarbitrary numberand broadcasts $\left[x_{k_{0,n+1}}.R'_{n+1}\right]$ to every earlier participantM_i of the group. On getting, they establish the fresh GK as

$$UJGK = (PGK)x_{K_{0,n+1}}R'_{n+1}.P = (\prod_{i=1}^{n+1} x_{K_{0i}}.R'_{n+1}).P$$

ii) The GC, S sends out $\left[(PGK)R'_{n+1}\right]P$ to M_{n+1}. Now M_{n+1} calculate the fresh key as

$$UJGK = (PGK)R'_{n+1}.x_{K_{0,n+1}}.P = (\prod_{i=1}^{n+1} x_{K_{0i}}R'_{n+1})P$$

Dynamic ExitProtocol



i) Once M_j wishes to exit the group, it informs the GC, S and then GC, Sgenerates R_j' a random number.

ii) Ssends $\left[R'_j x^{-1}_{K_{o,j}}\right]P$ to the respective member of the group M_i, $i?j$,(i.e), excluding exit participant.

$$S \xrightarrow{\left[R'_j x^{-1}_{K_{0,j}}\right]P} M_i, for 1 \le i \le n, i \ne j$$

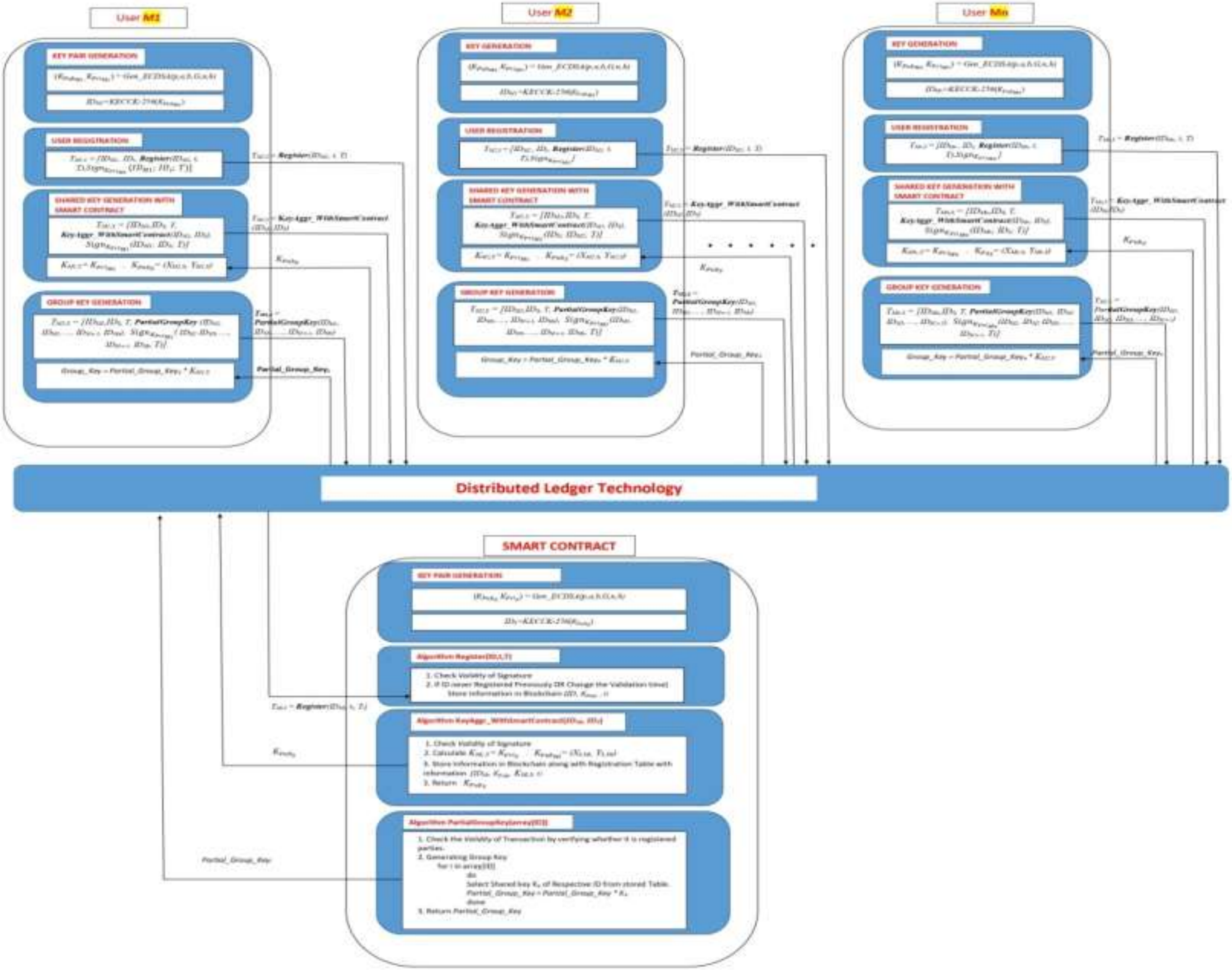
Subsequent to getting, each participant and calculate the updated- key as under.

$$ULGK = \left[x_K R'_j x^{-1}_{K_{0,j}}\right]P = \left[\prod_{i=1, i\ne j}^{n} x_{K_{0,i}} .R'_j\right]P$$ where??is PGK.

iii) The GC,Scomputes the updated key as follows.

$$ULGK = \left[x_K R'_j x^{-1}_{K_{0,j}}\right]P = \left[\prod_{i=1, i\ne j}^{n} x_{K_{0,i}} .R'_j\right]P$$ where??is PGK.

BACGKA-Protocol



User M1
User M2
User Mn
KEY PAIR GENERATION
KEY GENERATION
USER REGISTRATION
SHARED KEY GENERATION WITH SMART CONTRACT
GROUP KEY GENERATION
Register
Key-Aggr_WithSmartContract
PartialGroupKey
Partial_Group_Key
Group_Key = Partial_Group_Key * K
Distributed Ledger Technology
SMART CONTRACT
KEY PAIR GENERATION
Algorithm Register(ID,t,T)
Algorithm KeyAggr_WithSmartContract(ID, ID)
Algorithm PartialGroupKey(array[ID])

Algorithm Register(ID,t,T)

1. Check Validity of Signature
2. If ID never Registered Previously OR Change the Validation time) Store information in Blockchain (ID, K, t)

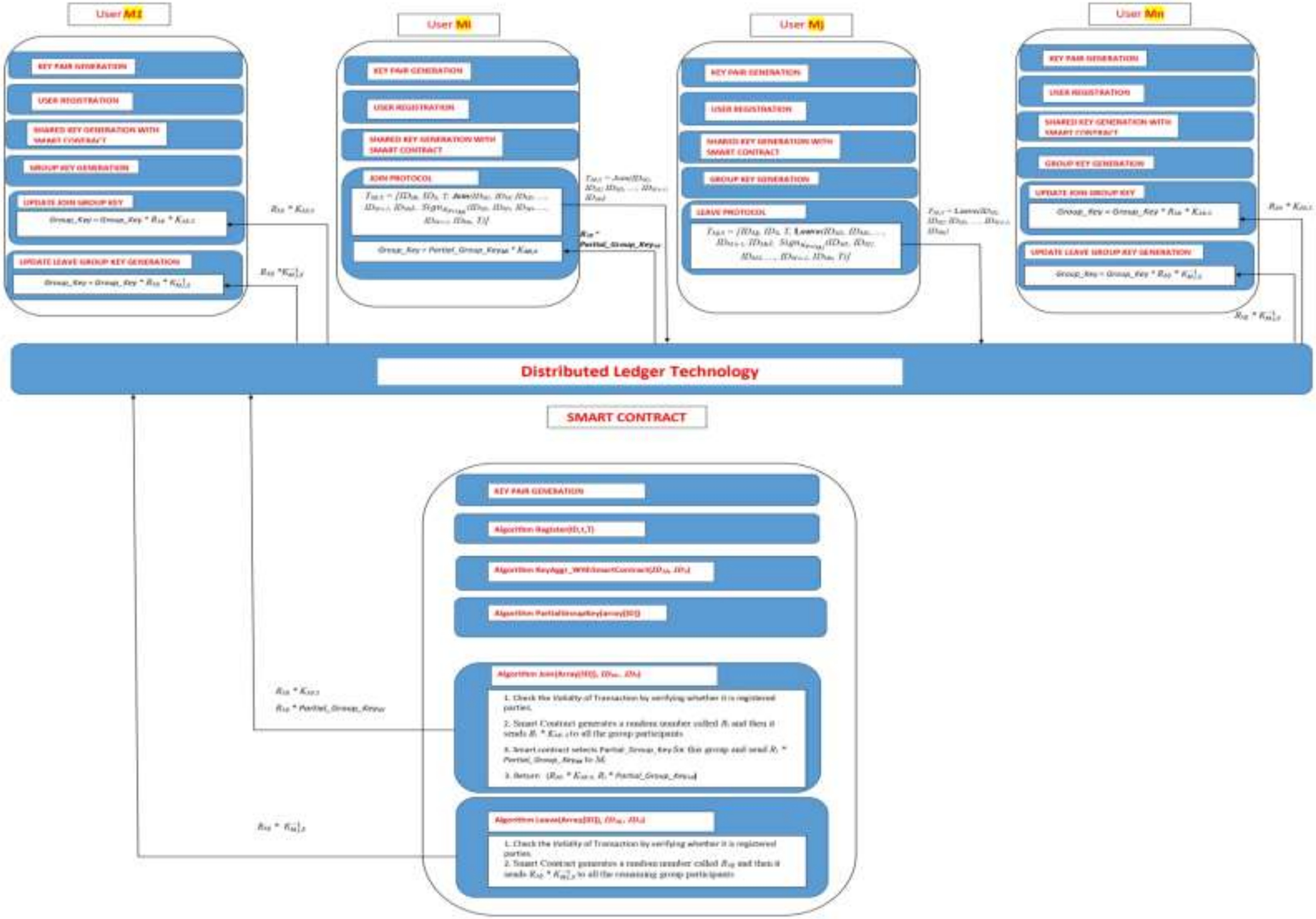
Algorithm KeyAggr_WithSmartContract(ID, ID)

1. Check Validity of Signature
2. Calculate K
3. Store information in Blockchain along with Registration Table with information (ID, K, K, t)
4. Return K

Algorithm PartialGroupKey(array[ID])

```
1. Check the Validity of Transaction by verifying whether it is registered parties.
2. Generating Group Key
      for i in array[ID]
            do
            Select Shared key K of Respective ID from stored Table.
            Partial_Group_Key = Partial_Group_Key * K
            done
3. Return Partial_Group_Key
```

BDACGKA-Protocol



User M1
KEY PAIR GENERATION
USER REGISTRATION
SHARED KEY GENERATION WITH SMART CONTRACT
GROUP KEY GENERATION
UPDATE JOIN GROUP KEY
$Group\_Key = Group\_Key * R_{SC} * K_{SM,1}$
UPDATE LEAVE GROUP KEY GENERATION
$Group\_Key = Group\_Key * R_{SC} * K_{M_j}^{-1}]_S$
$R_{SC} * K_{SM,1}$
$R_{SC} * K_{M_j}^{-1}]_S$
User Mi
KEY PAIR GENERATION
USER REGISTRATION
SHARED KEY GENERATION WITH SMART CONTRACT
JOIN PROTOCOL
$T_{M_i,S} = \{ID_{M_i}, ID_S, T, \textbf{Join}(ID_{M_1}, ID_{M_2}, ID_{M_3}, \ldots, ID_{M_{i-1}}, ID_{M_i}), Sign_{Key_{M_i}}(ID_{M_1}, ID_{M_2}, ID_{M_3}, \ldots, ID_{M_{i-1}}, ID_{M_i}, T)\}$
$Group\_Key = Partial\_Group\_Key_{M_i} * K_{SM,i}$
$T_{M_i,S} = Join(ID_{M_1}, ID_{M_2}, ID_{M_3}, \ldots, ID_{M_{i-1}}, ID_{M_i})$
$R_{SC} * Partial\_Group\_Key_{M_i}$
User Mj
KEY PAIR GENERATION
USER REGISTRATION
SHARED KEY GENERATION WITH SMART CONTRACT
GROUP KEY GENERATION
LEAVE PROTOCOL
$T_{M_j,S} = \{ID_{M_j}, ID_S, T, \textbf{Leave}(ID_{M_1}, ID_{M_2}, \ldots, ID_{M_{j-1}}, ID_{M_j}), Sign_{Key_{M_j}}(ID_{M_1}, ID_{M_2}, ID_{M_3}, \ldots, ID_{M_{j-1}}, ID_{M_j}, T)\}$
$T_{M_j,S} = Leave(ID_{M_1}, ID_{M_2}, ID_{M_3}, \ldots, ID_{M_{j-1}}, ID_{M_j})$
User Mn
KEY PAIR GENERATION
USER REGISTRATION
SHARED KEY GENERATION WITH SMART CONTRACT
GROUP KEY GENERATION
UPDATE JOIN GROUP KEY
$Group\_Key = Group\_Key * R_{SC} * K_{SM,n}$
UPDATE LEAVE GROUP KEY GENERATION
$Group\_Key = Group\_Key * R_{SC} * K_{M_j}^{-1}]_S$
$R_{SC} * K_{SM,n}$
$R_{SC} * K_{M_j}^{-1}]_S$
Distributed Ledger Technology
SMART CONTRACT
KEY PAIR GENERATION
Algorithm Register(ID,t,T)
Algorithm KeyAggr_WithSmartContract(ID_{Mi}, ID_S)
Algorithm PartialGroupKey(array[ID])
Algorithm Join(Array[ID], ID_{Mi}, ID_S)
Algorithm Leave(Array[ID], ID_{Mj}, ID_S)
$R_{SC} * K_{SM,i}$
$R_{SC} * Partial\_Group\_Key_{M_i}$
$R_{SC} * K_{M_j}^{-1}]_S$

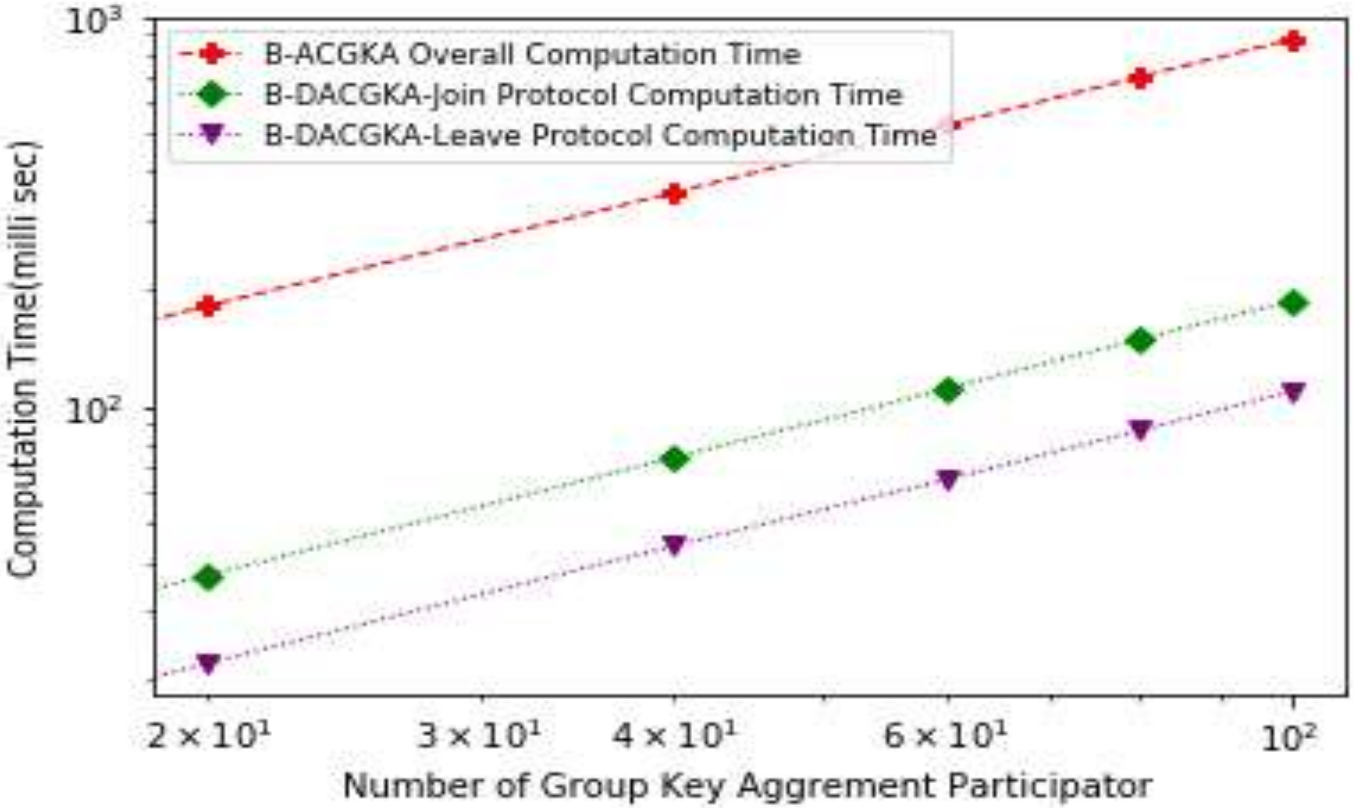
Algorithm Join(Array[ID], ID_{Mi}, ID_S)

1. Check the Validity of Transaction by verifying whether it is registered parties.
2. Smart Contract generates a random number called R_i and then it sends $R_i * K_{SM,i}$ to all the group participants
3. Smart contract selects Partial_Group_Key for this group and send R_i * $Partial\_Group\_Key_{M_i}$ to M_i
3. Return $(R_{SC} * K_{SM,i}, R_i * Partial\_Group\_Key_{M_i})$

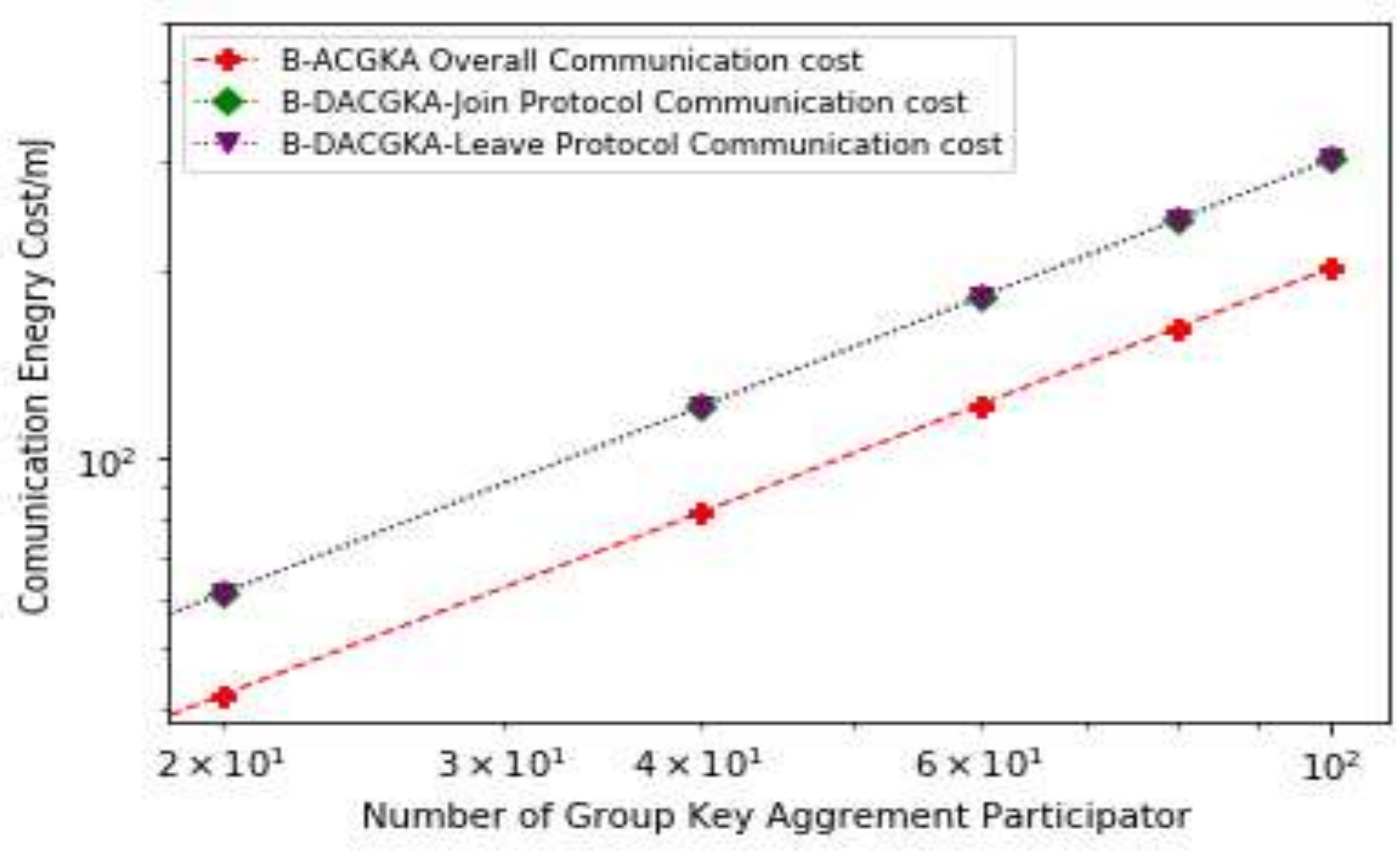
Algorithm Leave(Array[ID], ID_{Mj}, ID_S)

1. Check the Validity of Transaction by verifying whether it is registered parties.
2. Smart Contract generates a random number called R_{SC} and then it sends $R_{SC} * K_{M_j}^{-1}]_S$ to all the remaining group participants

Computation



Communication



Contributions/ Highlights of the work:

- The core contribution of the paper is to build a Provably Secure BlockchainSmart Contract Centric Group Key Agreement for Large Wireless Ad-Hoc Networks comprising the following
- An inbuilt **anonymous identity authentication**to protect personal privacy. .
- **Computation Efficiency**:The computation overhead of GKA can be distributed and different node to attain load balancing and to diminish the computation load on a single node.
- Further the major computation load in the proposed protocol will be the burden of smart contract which can made it easy because of the computation efficiency and the remaining group members will have very less computation requirement made our protocol efficient.
- Since smart contract place a GC role in contrast to exiting GC based key agreement protocols there is no question of single point failure and compromise made our protocol secure and efficient.

- **Communication Efficiency**: Being a Blockchain based in contrast to exiting GKA, the proposed protocol highly reduces the communication complexity.
- **Dynamic Nature:** DGCGKA to address join or leave of a participant from the group with forward and backward secrecy. Further in contrast to exiting GC based key agreement protocols, the proposed protocol having smart contract as GC there is no question of GC leaving which can be a greater burden to choose the another member as a GC.
- **Trust:** Apart from trust in blockchainthe proposed protocol no member can't influence entire group key because of contributory nature of the group key. Further with hashing mechanism of Blockchain Technology. Moreover, we established formal security model for the proposed protocol.

- **Traceability and Accountability:** Any malicious participant attempt to disrupt the establishment of GKA can be easily detected and will be tracked.
- **Adaptability to Large WANETS:** The proposed protocol being ECDH, light weight and decentralized could be easily adaptable to ad-hoc networks such as WANET, MANET.
- **Disintermediation:** Using Blockchain Technology, Group members can exchange the data without involving the third party for establishment of trust.

Thank You!

Module-2

A Presentation

on

How to Publish Quality Research

BY

Dr.V Srinivas Naresh,

M.Tech., Ph.D., CSIR-JRF.

Associate Dean Research and Development

Contents Of Presentation

Types of Research Papers

Quality of Journal

✓Indexing

✓Publisher

✓Measures: Impact Factor, H index

Selection of Journals

✓Journal Finders

Paper Submission

Review Process

Types of Research Paper

- Short Communication
- Review Paper
- Full Articles

Research Paper

- Short Communication: (LETTERS/RAPID COM Length 2 pages)
  - if you are working with **a *hot topic and had discovered something never explored before in the literature***.
  - This is done to ensure that you are the ***first scientist to report this feature.***
  - In some research topic thing go very fast and in some weeks another author can publish what you have discovered!
  - Normally a communication need to be about a really ***novel feature***!
  - https://www.quantifiedcommunications.com/blog/artificial-intelligence-in-communication

Research Paper

- Review Paper:
  - The purpose of a review paper is to briefly ***review recent progress in a particular topic***.
  - Overall, the paper summarizes the current state of knowledge of the topic.
  - It creates an ***understanding*** of the topic for the reader by discussing the ***findings presented in recent research papers.***
  - A review paper is not a "term paper" or book report. It is not merely a report on some references you found.
  - Instead, a review paper synthesizes ***the results from several primary literature papers*** to produce a coherent argument about a topic or focused description of a field.

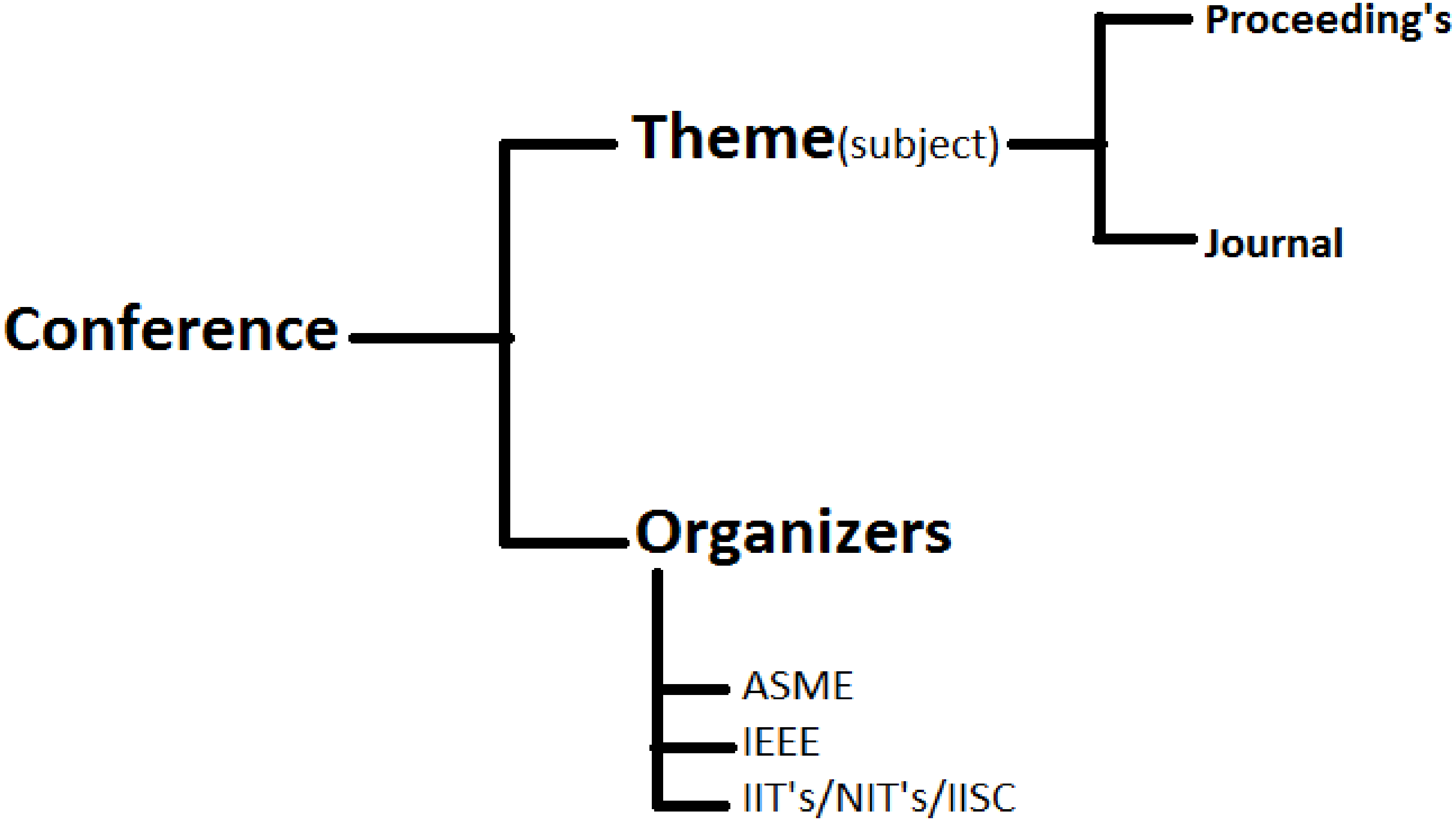
https://link.springer.com/article/10.1007/s40032-016-0289-y

Research Paper

Full Articles:

- This is the most common type of journal manuscript used to publish full reports of data from research.
- It may be called an ***Original Article****, Research Article, Research,* or just *Article,* depending on the journal.
- The **Original Research** format is suitable for many different fields and different types of studies.
- It includes full Introduction, Methods, Results, and Discussion sections.

Quality of Conference



Conference

Theme(subject)

Proceeding's

Journal

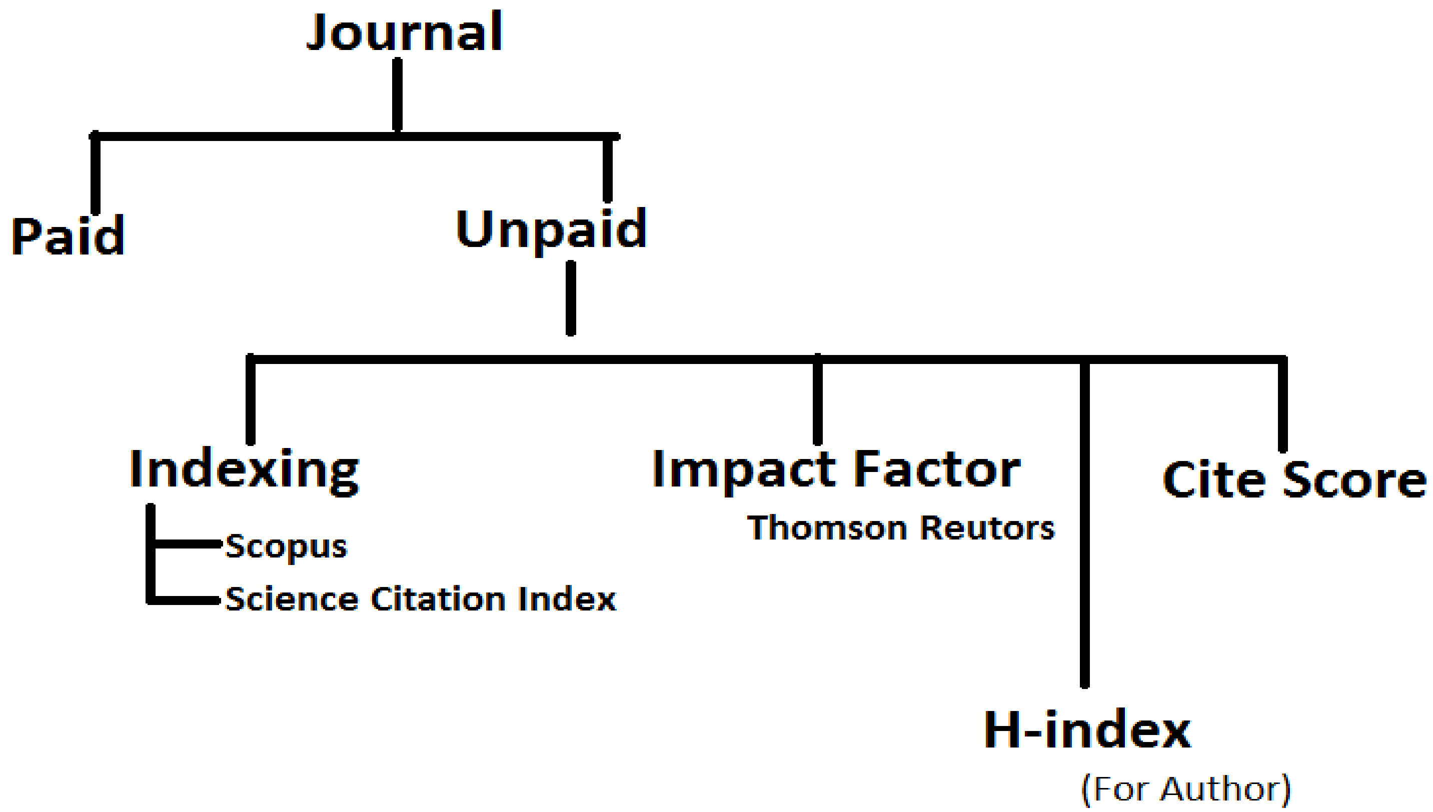
Organizers

ASME

IEEE

IIT's/NIT's/IISC

Quality of Journal



Journal

Paid

Unpaid

Indexing

- Scopus
- Science Citation Index

Impact Factor

Thomson Reutors

Cite Score

H-index

(For Author)

Quality of Journal

- What is ISI?
  - ISI is the Institute for Scientific Information (ISI) was founded by Eugene Garfield in 1960.

❑How to find the impact factor and rank for a journal?

✓Journal Citation Report (JCR) ***Impact Factor*** – ISI Thompson (beware of another ISI impact used by predatory journals) -SCI, SSCI, SCIE, ESCI https://clarivate.com/webofsciencegroup/wp-content/uploads/sites/2/dlm_uploads/2019/08/JCR_Full_Journal_list140619.pdf

✓***SJR,SNIP,H-index*** – Scopus

Quality of Journal

- The ISI Web of Knowledge suite encompasses the following databases:
  - Science Citation Index (SCI)
  - Science Citation Index Expanded (SCIE)
  - Emerging Source Citation Index (ESCI)
  - Biological Abstracts
  - Biosis Citation Index
  - Current Chemical Reactions
  - Current Contents Connect
  - Index Chemicus
  - BIOSIS Citation Index

http://en.wikipedia.org/wiki/ISI_Web_of_Knowledge#Abstracting_and_indexing

Quality of Journal

- Top Three Indexes
  - Science Citation Index Expanded (Larger version of SCI) covers more than 6,500 notable and significant journals
  - Arts and Humanities Citation Index, which covers 1130 journals, beginning with 1975.
  - Social Sciences Citation Index, which covers 1700 journals, beginning with 1956.

http://en.wikipedia.org/wiki/Science_Citation_Index

Example

http://ip-science.thomsonreuters.com/mjl/

http://science.thomsonreuters.com/cgi-bin/jrnlst/jloptions.cgi?PC=K

Quality of Journal

- Impact Factor:

- The **JCR** provides ***quantitative tools for ranking, evaluating, categorizing, and comparing journals***.
- The impact factor is one of these; it is a measure of the frequency with which the "average article" in a journal has been cited in a particular year or period.
- The annual JCR impact factor is a ratio between citations and recent citable items published.
- Thus, the impact factor of a journal is calculated by dividing the number of current year citations to the source items published in that journal during the previous two years.

- Calculation for journal impact factor.

A= total cites in 1992

B= 1992 cites to articles published in 1990-91(this is a subset of A)

C= number of articles published in 1990-91

D= B/C = 1992 impact factor

Quality of Journal

- Impact Factor:
  - List of Impact Factor Journal from JCR:
    - We cannot get the list of IF journal from JCR (ISI-Thomson) directly. Alternatively, we can get it through the address below:
    - http://www.bioxbio.com/if/html/

Quality of Journal

- Scopus Quality Measures:
- **SJR - SCImago Journal Rank**
- https://www.scimagojr.com/journalsearch.php?q=21100200832&tip=sid
- ***SJR calculation***

# citations received in a year

÷

# of documents published in previous 3 years

SNIP

- **SNIP (Source Normalized Impact per Paper) Calculation**

journal's citation count

÷

citation potential in its subject area

h index

- The h index Expresses the journal's number of articles (*h*) that have received at least h citations. It quantifies both journal scientific productivity and scientific impact and it is also applicable to scientists, countries, etc. Author's total article count = 33
- 18 of the articles are cited at least 18 times
- h-index = 18

CiteScore

- **CiteScore** is the number of citations received by a journal in one year to documents published in the three previous years, divided by the number of documents indexed in Scopus published in those same three years.
- CiteScore for 2015 counts the citations received in 2015 to documents published in 2012, 2013 or 2014, and divides this by the number of documents published in 2012, 2013 and 2014.

Selection of Journal

- Do all journals charge publishing fee to authors?
  - NO!!!
- Reputable publishers (IEEE, Elsevier, Springer, Wiley, Tailor &Francis, etc.) usually offer two options to authors: open access vs non open access
- If we choose an open access mode, we have to pay some money to publisher
- Some publishers also offer open access mode with free of charge (usually affiliated with university)
- Knowledge Management & E-Learning (KMEL), Journal of Theoretical and Applied Electronic Commerce Research (JTAER), Electronic Journal of University of Malaya (Malaysian Journal of Computer Science, Malaysian Journal of Library & Information Science, etc.,), International Journal on Smart Sensing and Intelligent Systems, etc.,
- Recommended publishers for beginner(free publishing fee and easier to accept) Inderscience.
- IGI Global

Points to be Considered before Publishing

- Targeted audience
- Prestige of journal and your own institution
- Access (open access/ subscribed)
- availability free of charge on the World Wide Web
- On payment
- Impact factor of the journal
- Probability of acceptance
- Publication time

Journal Finders

- Springer
  - https://journalsuggester.springer.com/
- Elsevier
  - https://journalfinder.elsevier.com/
- John Wiley
  - https://journalfinder.wiley.com/search?type=match
- Taylor and Francis

Paper Submission:

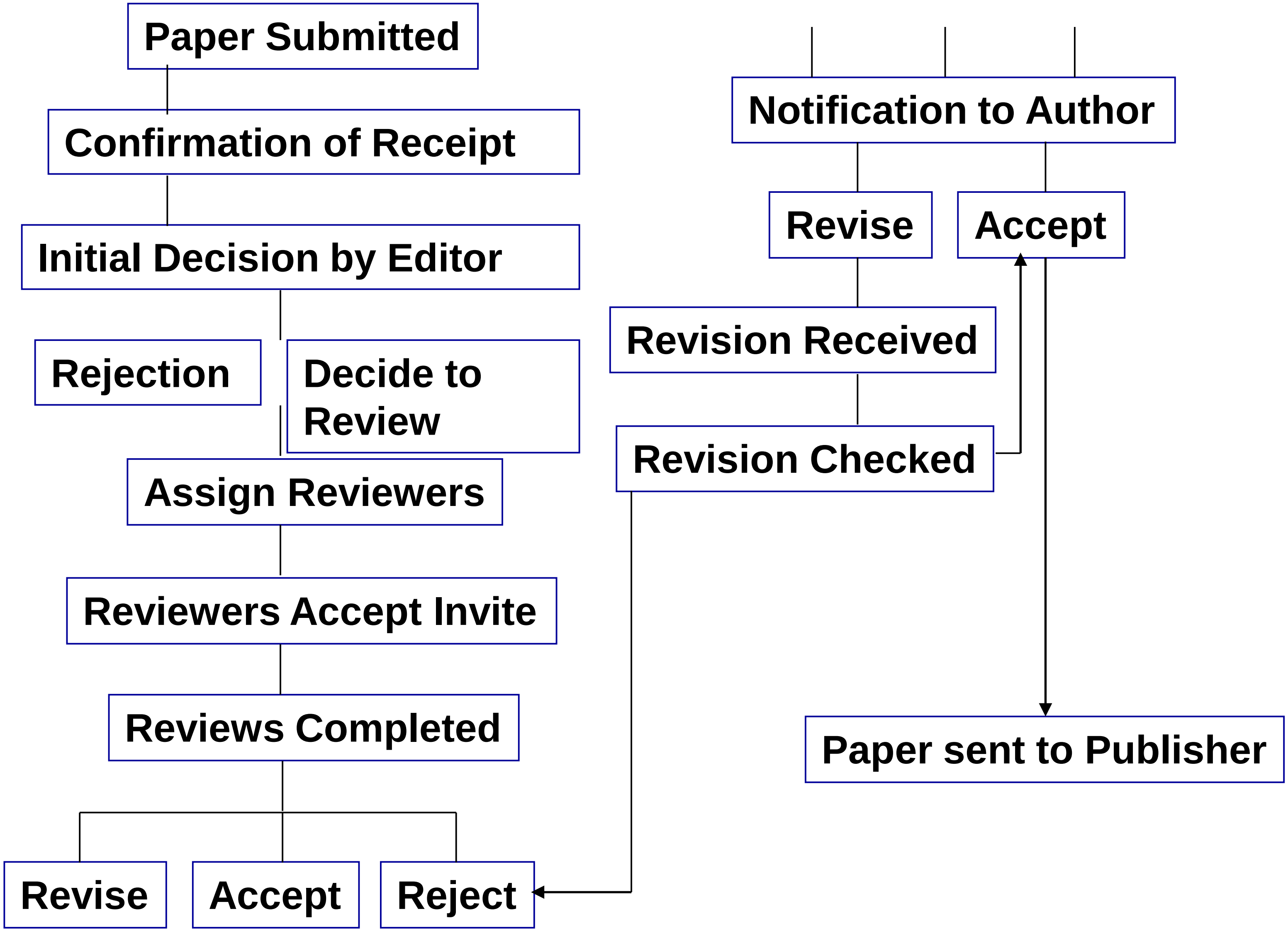
Before Submission

- Read the instructions for authors carefully
- Format manuscript in line with the journal style
- https://www.overleaf.com/project/5d8e2fdfc56033000146fe12
- Send the manuscript to the journal editor and await for the acknowledgement
- Wait for reviewers comments
- Address all the comments of the reviewers

After Submission

- Most journal editors will make an initial decision on a paper - to review or to reject
- Most editors appoint two referees
- Refereeing speed varies tremendously between journals
- Authors should receive a decision of Accept, Accept with Revision (Minor or Major), or Reject
- If a paper is rejected, most editors will write to you explaining their decision
- After rejection, authors have the option of submitting the paper to another journal - editor’s suggestions should be addressed

Overview of Peer Review Process



Paper Submitted

Confirmation of Receipt

Initial Decision by Editor

Rejection

Decide to Review

Assign Reviewers

Reviewers Accept Invite

Reviews Completed

Revise

Accept

Reject

Notification to Author

Revise

Accept

Revision Received

Revision Checked

Paper sent to Publisher

What to do if a paper gets rejected

- What to do if a paper gets rejected……
- ***Do not get discouraged***. Read editorial comments and discuss with advisor/students/collaborators. Find out how you can make this study stronger and acceptable for publication.
- ***Do not just turn around*** and submit the paper to another journal. Read carefully the comments and find ways to improve the scientific quality of the papers
- Carry out additional experiments and ***improve the quality of scientific discussions.*** (Journals often look for papers with quantitative and mechanistic information that represent new physical insights)
- Rejected papers can be resubmitted if and only the concerns of the reviewers are adequately addressed and new results are included.
- If you have questions, please feel free to contact the editorial office.

My Experiences in Publishing Quality Research: A Case Study

- https://www.researchgate.net/profile/Vankamamidi_Srinivasa_naresh/publications

ORIGIN OF MY RESEARCH-DH

- IDEA: CHANGING KEYS- MSK
- IDEA:EXTENDING TO N-PARTY-GKA
- IDEA:FOR AD-HOC NETWORKS-EC-MSK
- IDEA:EC-GKA
- IDEA:EC-GKA-PKI
- IDEA:EC-GKA-WITH-DIG SIGNATURE
- IDEA:HEC-DH
- HEC-GKA
- CLUSTER BASED HEC-DH
- HEC-BASED-MSK

Thank you