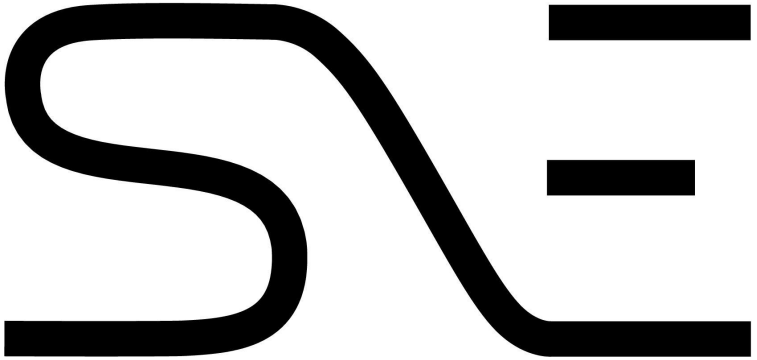
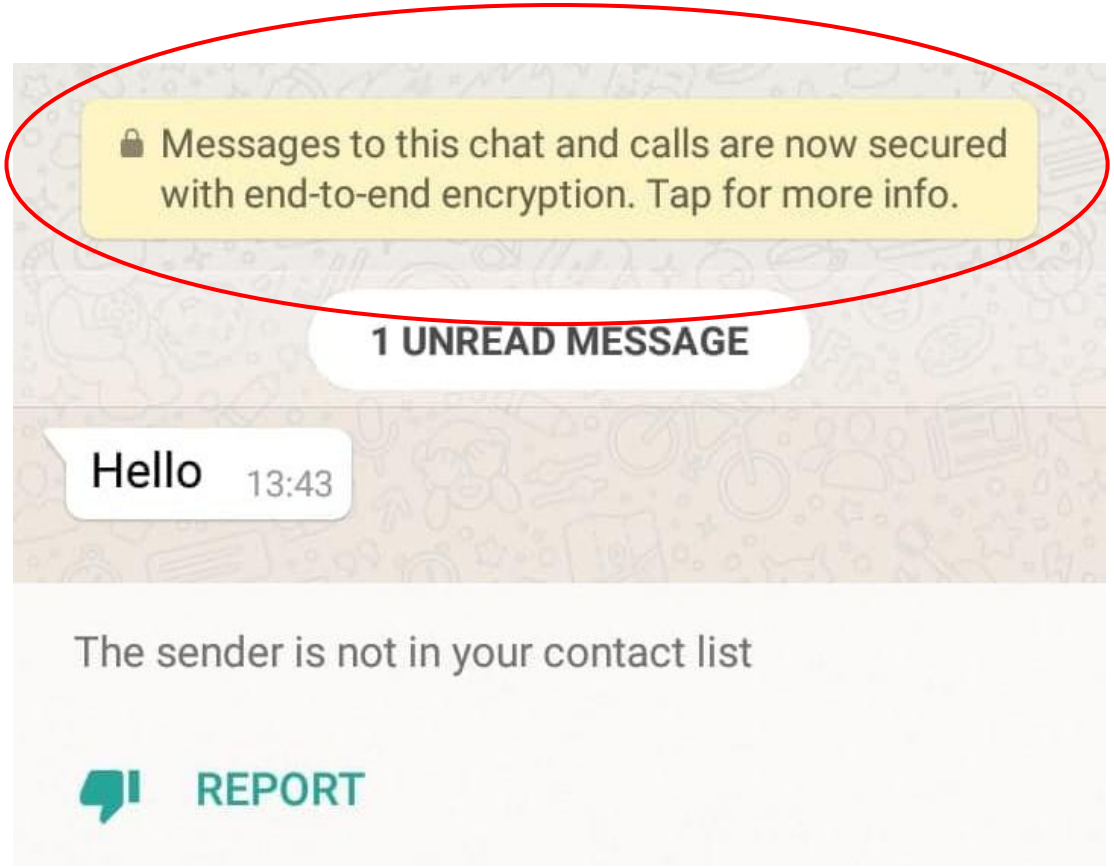


WhatsApp End-to-End Encryption: Are Our Messages Private?

Research project by:
Pavlos Lontorfos
Tom Carpaij

Supervisors:
Ruben De Vries
Soufiane el Aissaoui

Introduction



Introduction

- 1.5 billion users
- “Black box” application
- Security vs. end-to-end encryption
- Can we trust Facebook's claim of End-to-End encryption?

Research questions

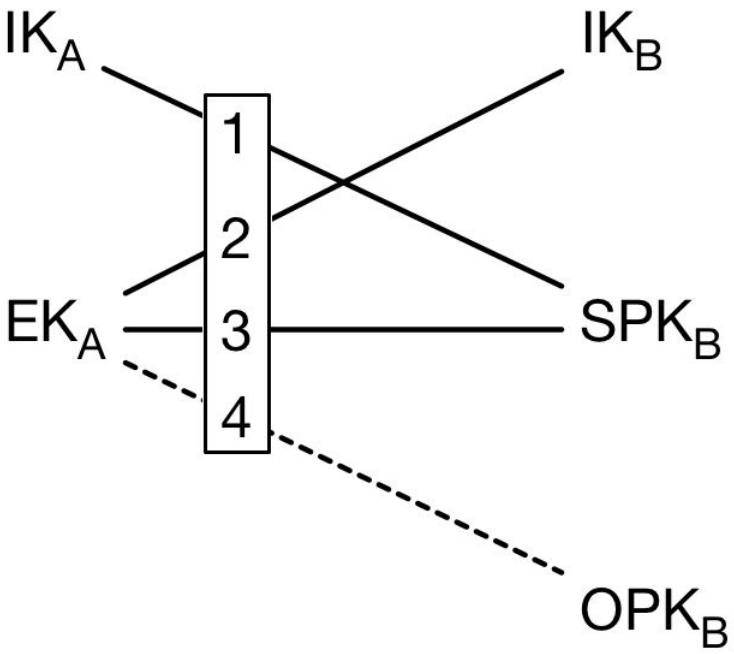
Is user-to-user message exchange via WhatsApp End-to-End encrypted?

- What are the algorithms used to create the Signal protocol?
- What are the differences between Signal and WhatsApp network traffic?
- To what extent are WhatsApp messages encrypted to the Signal protocol specifications?

Literature review

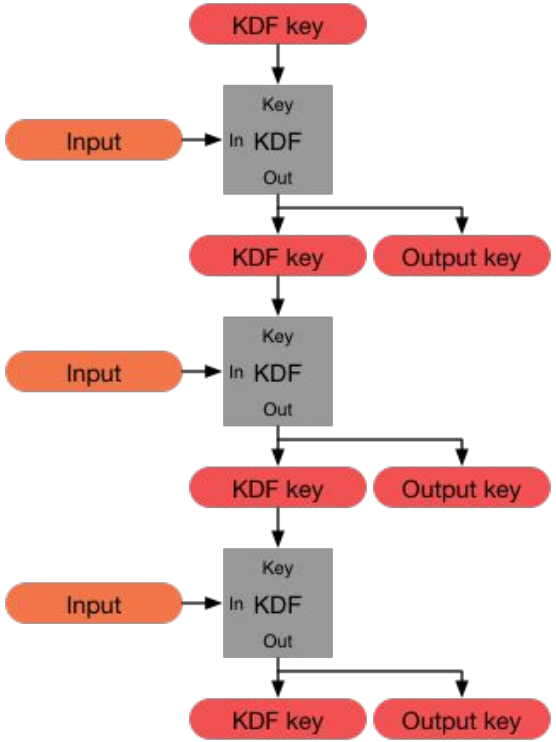
- Breach of End-to-End encryption in group messages [1]
- Non-blocking WhatsApp implementation [2]
- Voicemail account verification hijack [3]
- Signal protocol papers [4] [5]
- WhatsApp End-to-End encryption implementation whitepaper [6]
- Formal proof of Signal protocol security [7]

Background: Extended Triple Diffie-Hellman (X3DH)



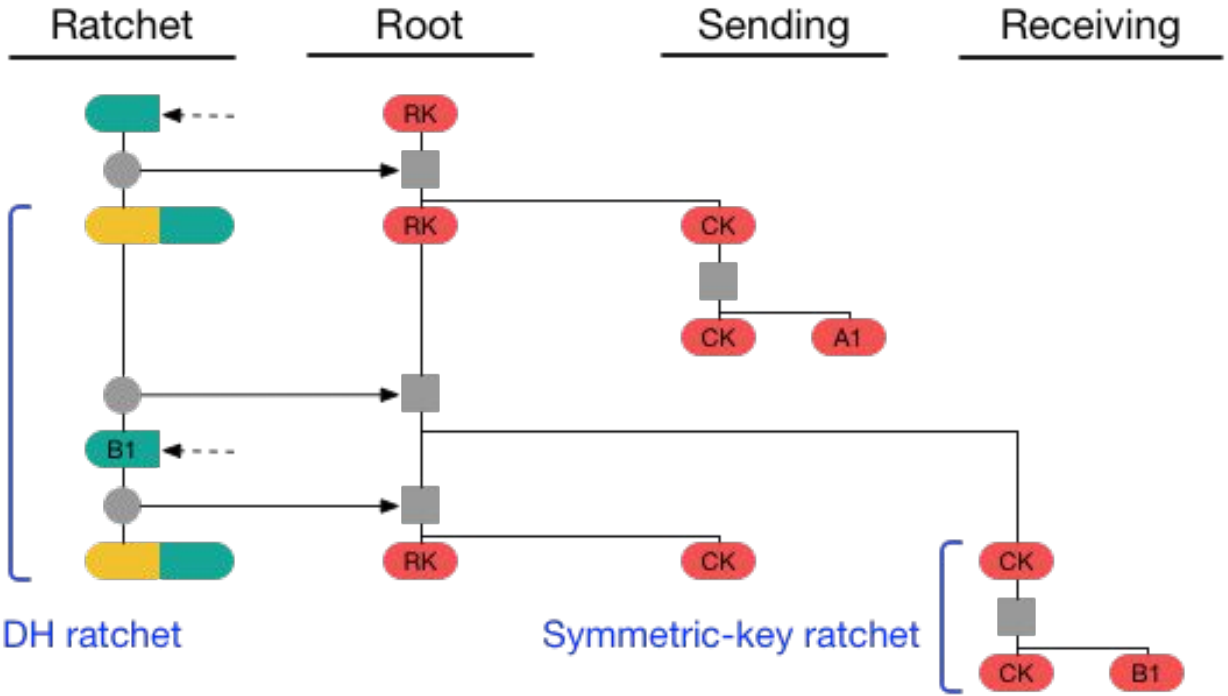
X3DH illustration. From *Open Whisper Systems*, by Marlinspike and Perrin, 2016.
Retrieved from https://signal.org/docs/specifications/x3dh/

Background: Single ratchet algorithm



Single ratchet illustration. From *Open Whisper Systems*, by Perrin and Marlinspike , 2016. Retrieved from https://signal.org/docs/specifications/doubleratchet/

Background: Double ratchet algorithm



Double ratchet illustration. From *Open Whisper Systems*, by Perrin and Marlinspike , 2016. Retrieved from https://signal.org/docs/specifications/doubleratchet/Set3_2.png

Blocking-Non blocking mechanism

Signal: Blocking Mechanism

- No message retransmission
- Smaller User Base
- Secure

WhatsApp: Non-blocking Mechanism

- Messages are retransmitted
- Friendly user experience/ convenience
- Security issues - Attack scenario

Methods

Assumptions made:

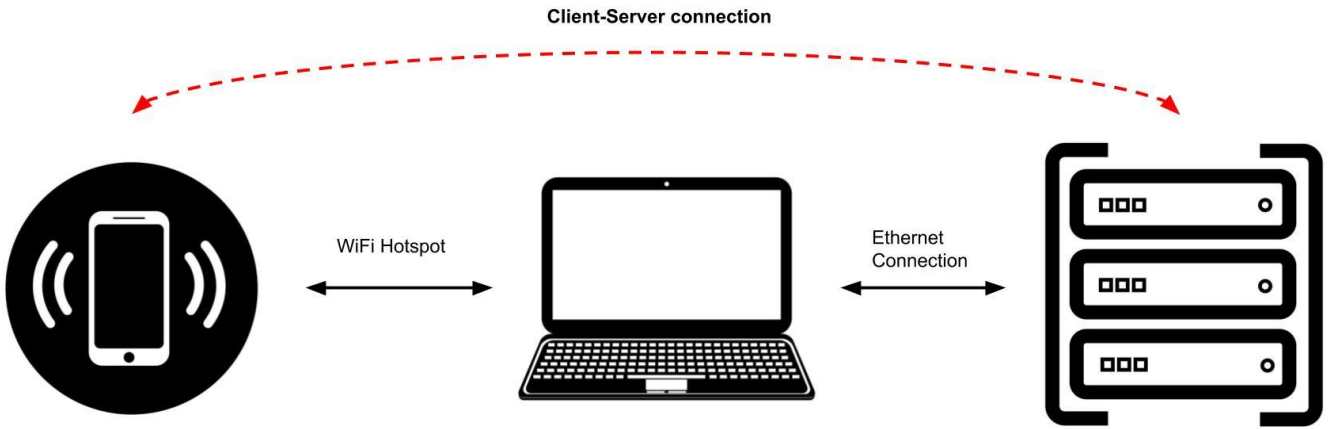
- If Signal is implemented correctly, the protocol is secure
- Signal Application implements their protocol correctly

WhatsApp is proprietary software

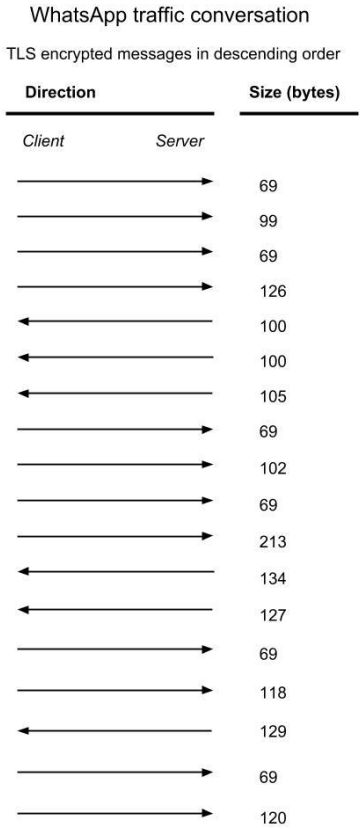
Android version was analyzed. Protocol implementation remains the same for IOS

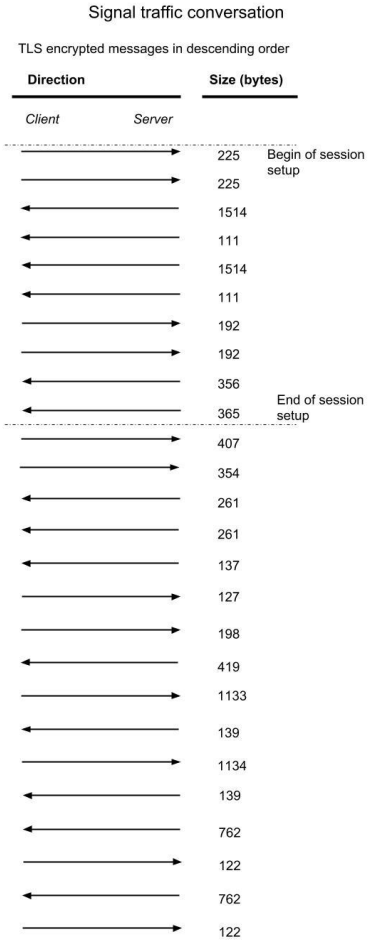
Latest available version of WhatsApp(2.18.380) and Signal(4.32.8)

Experiments

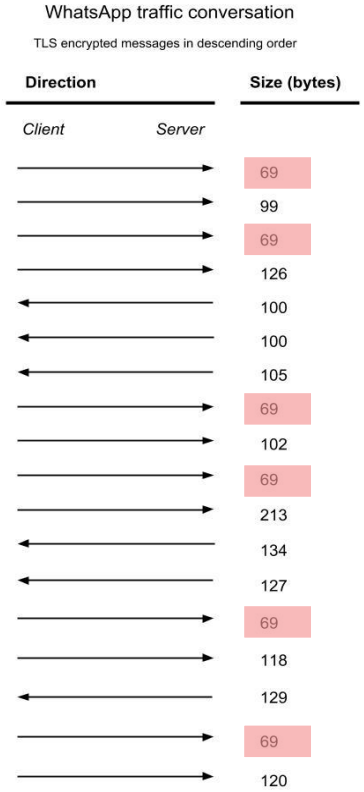


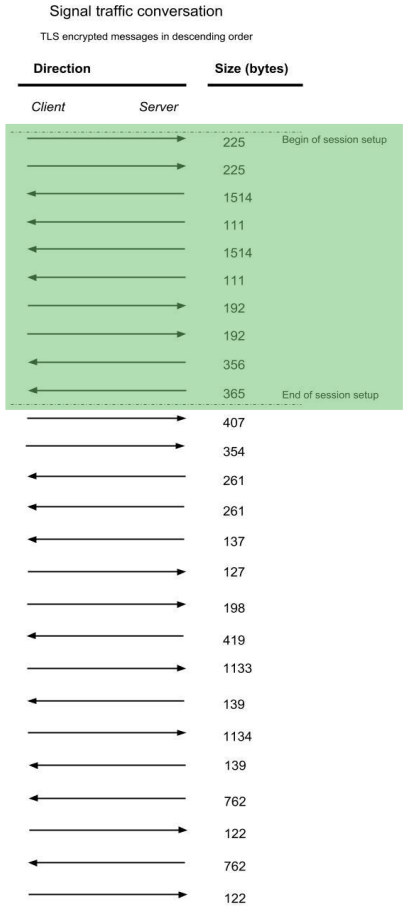
Experiment: Traffic comparison



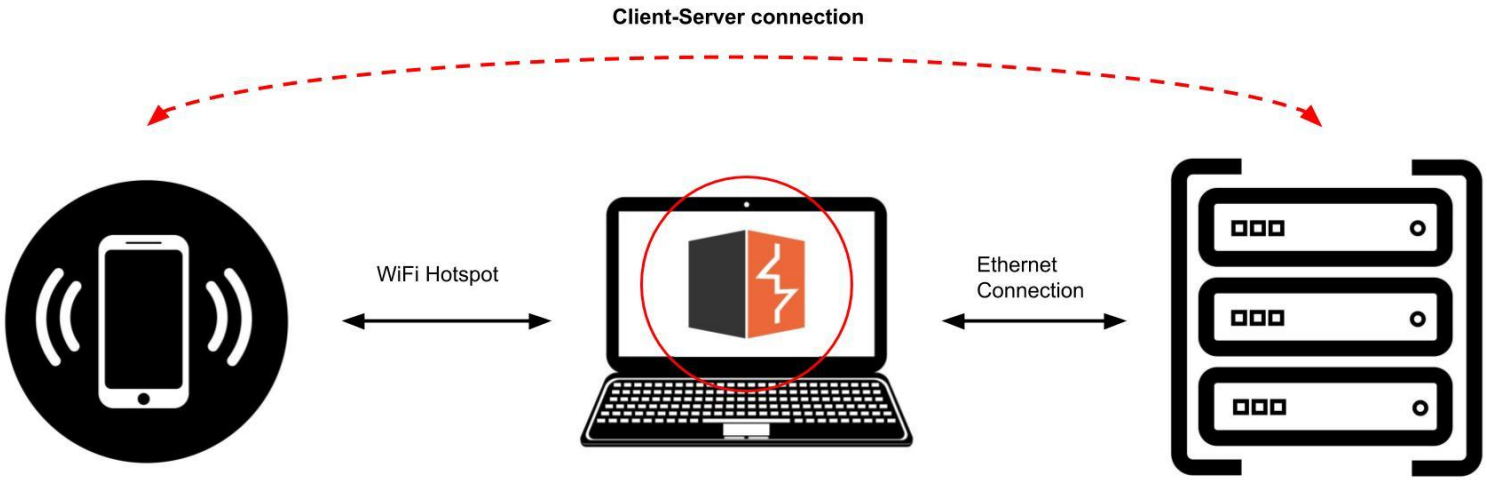


Results: Traffic comparison





Experiment: Packet decryption



Results: Packet decryption

Raw | Params | Headers | Hex

```
PUT /v1/messages/+306937299980 HTTP/1.1
Unidentified-Access-Key: +no5WT1wgHn8kh06jfTJdg==
X-Signal-Agent: OWA
Content-Type: application/json; charset=utf-8
Content-Length: 898
Host: textsecure-service.whispersystems.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.9.0

{"destination":"+306937299980","messages":[{"content":"EQohBc0EfHYN+k7zrfRNa6/oxca9ignEcTP8FwG4vu9UeKBLEisqZ+h9yrBnwzlDe09QqKDedbegl5uRe2/BJRX5BgGnGxg8ZxmaUWo+7TjFGtEDZtSxmuh0Nf
VfF2HP8kqCDwRCY6urXulLThCSxvYn/AUjZ8kLWV26HhNYzbDN1sRfMb+HxCSAI0EXQ/LQVkFLLCSZwD197QoFHtYTDhSOfkHPseBEon5S0eB+xTKVywef8B/y2HsRTv4yVcXn4euy85wnH9/UdhjBcgCFOI+87qP6dSK6d2Kt3I9ewBS
SlL76Bk2nt2cTimORmXymaWux1DYFSEIS0sIWl/F1bxKnZ+YranOu/e2Ps7fjINyscw2xLtvqERw2R0loOor1raGG0zA5BzVm0mzt8oZJUXi1RHQUOGVq46vGuVmYs6hDOtPNegZYaJ3ZXdzn99jyzNzGsaT5+St0HoFJzhctxteX8RcL
wxhgBY7w8P0jjd9H0D3HG54xi7JPlGuPlHqXA5I/UsqwkYpJEW3v/CJM6rIgL3exmKO/Vkpm7FDEx+wwFQlTJwA9kC4DZsDy6+iupX6iFdcKKjb1faV6aEOcMKC7z69hnbsOjxBpUYiIRofEkW74tQmhblq/rweuaBzVyPIXHoWtLdjix
XK074X6gtQIUjrOUK628uYWFCgl7ZaODBkLKf+6x8MWIOaO7mYXpOYhgi5mxZzPrWKZhG4+l4vRRaKt","destinationDeviceId":1,"destinationRegistrationId":16356,"type":6}],"online":true,"timestamp":1
548771435261}
```

Results: Packet decryption

```
GET /v1/websocket/?login=+31647229265&password=twqrl/6AmDskyse3mqQDxtaR HTTP/1.1
X-Signal-Agent: OWA
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Key: s5Q7IWYO08+06EbkKQxQsw==
Sec-WebSocket-Version: 13
Host: textsecure-service.whispersystems.org
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.9.0
```

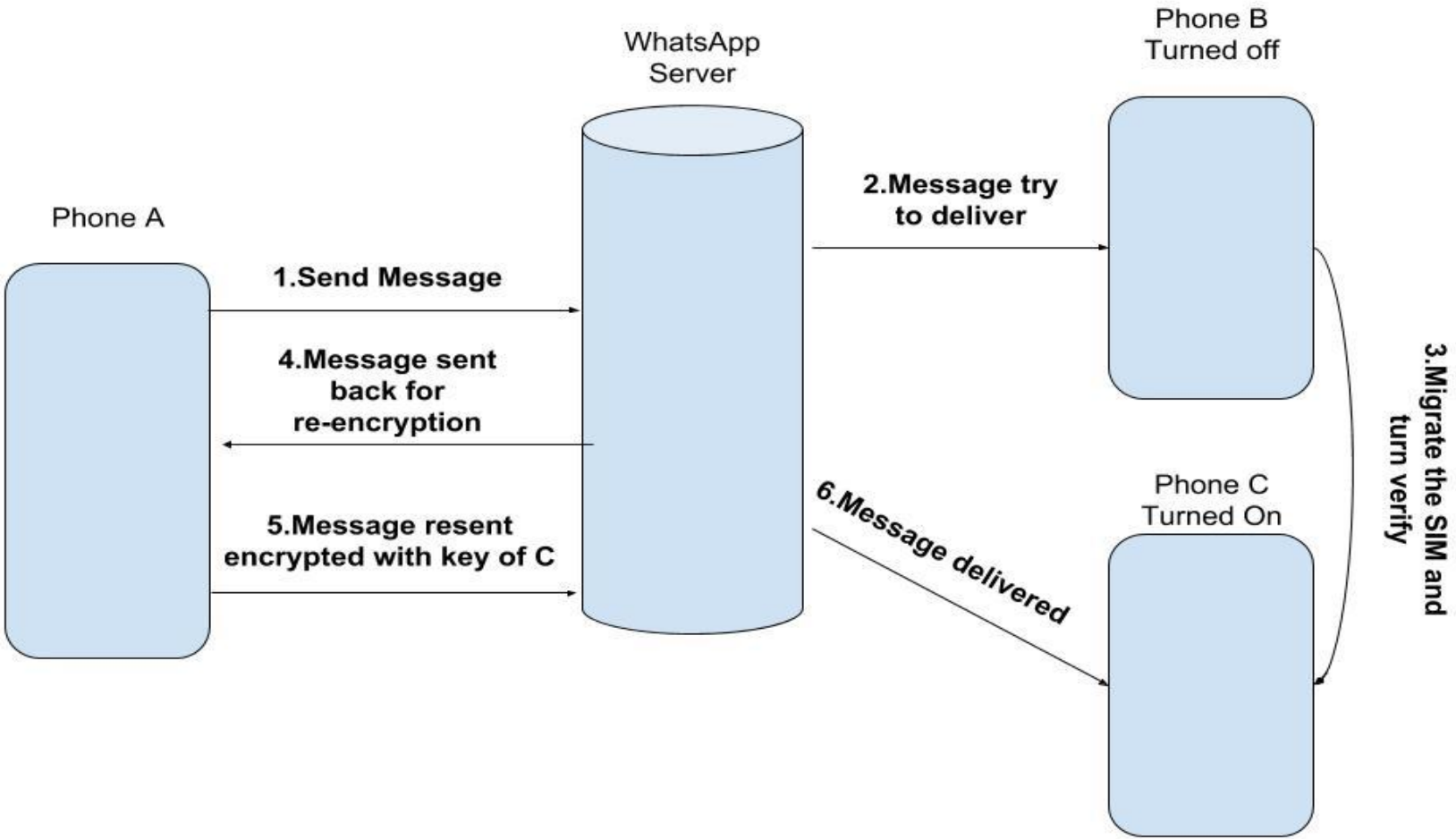
Results: Packet decryption

Unfortunately no packets captured from WhatsApp

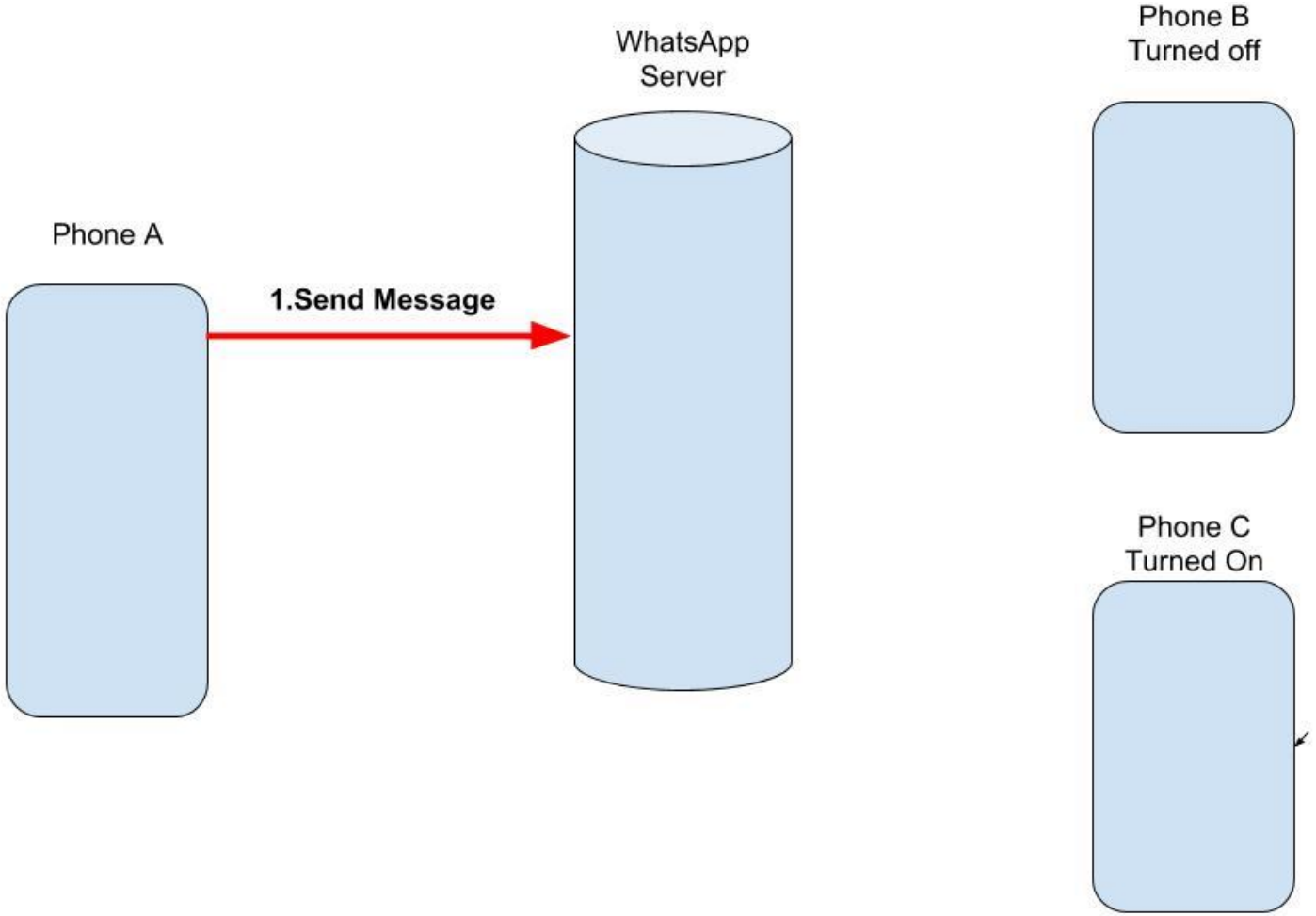
Noise Pipes : Custom protocol instead of TLS

Burp Suite couldn’t recognise those packets

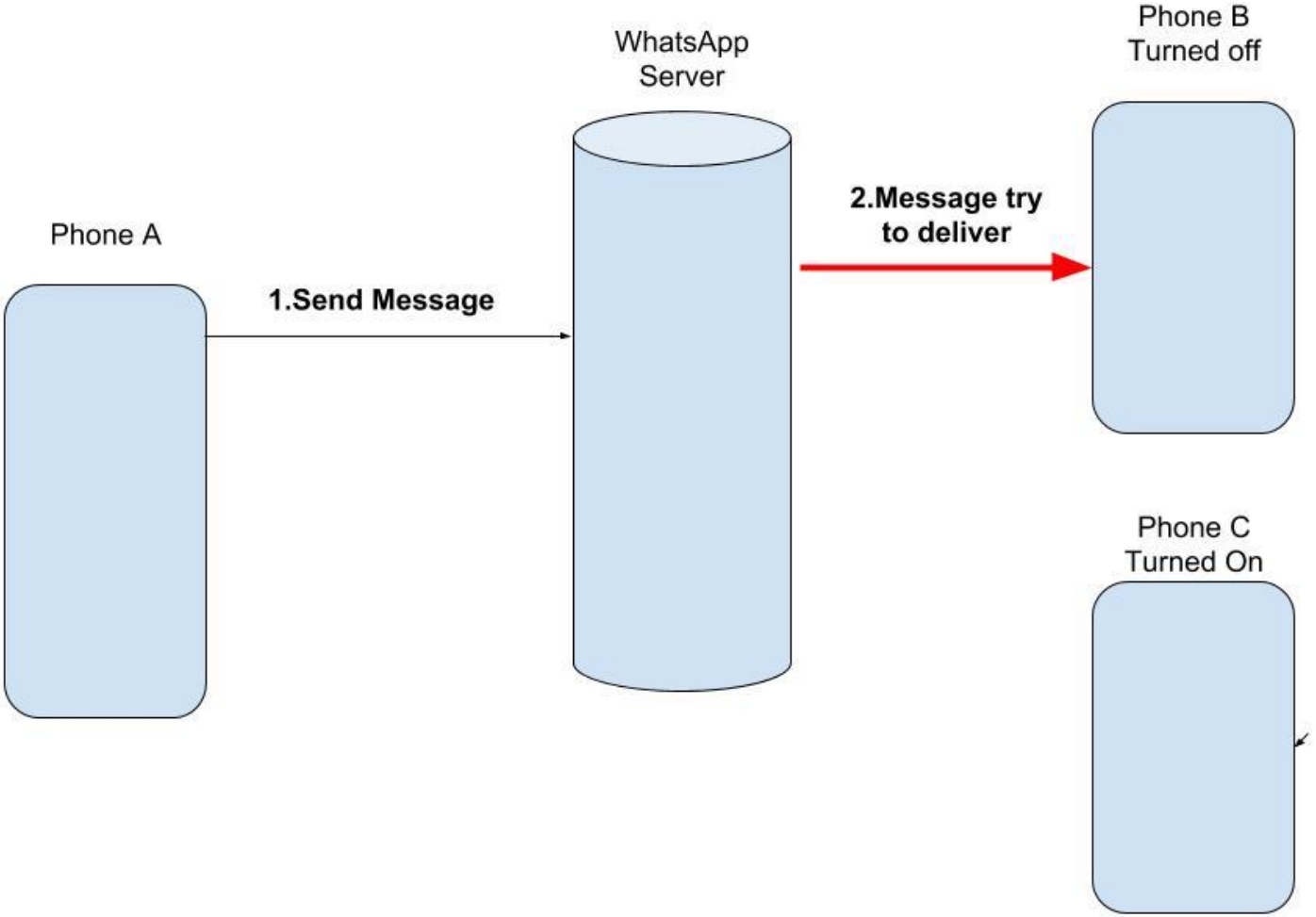
Experiment: Basic blocking



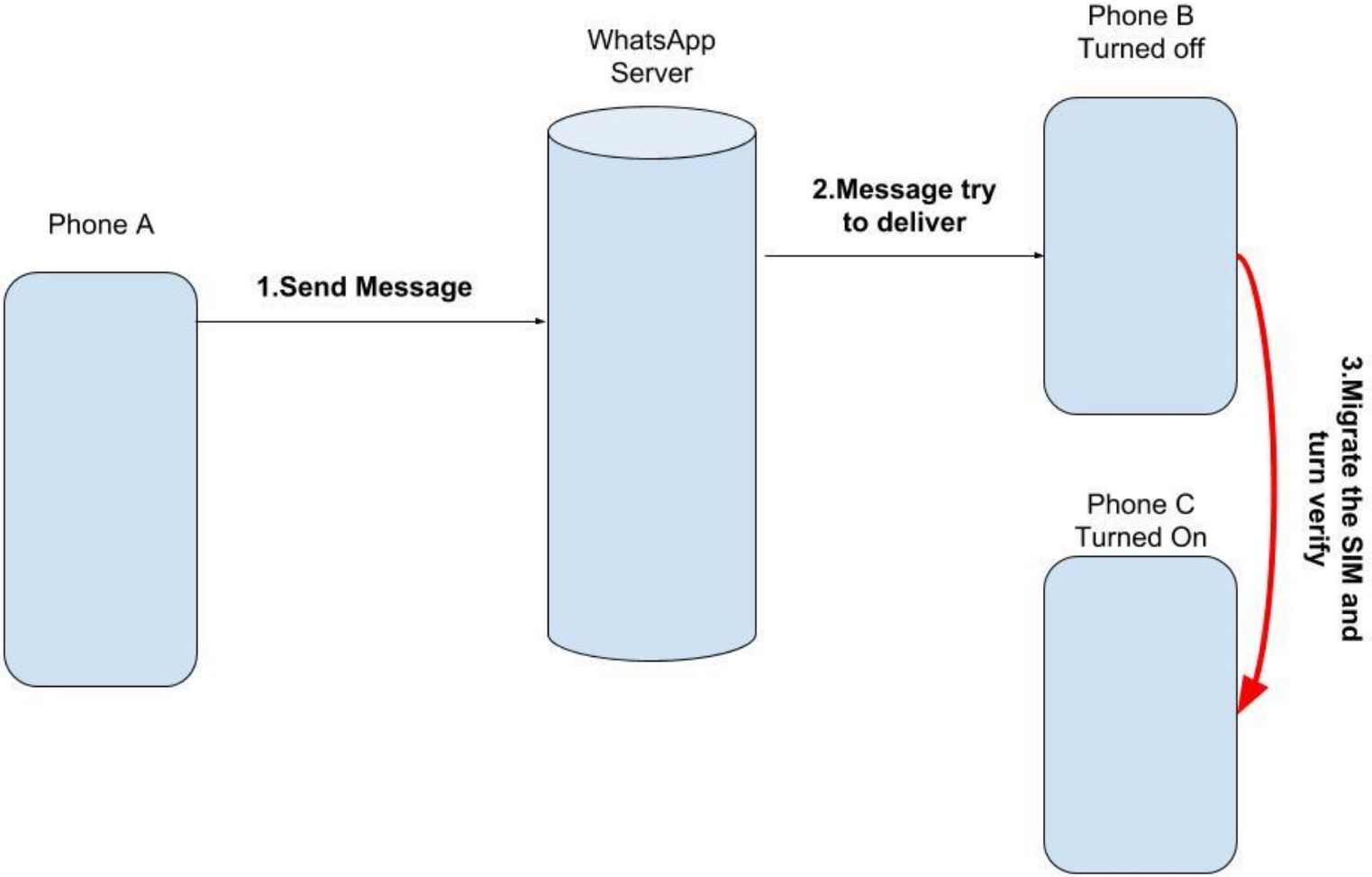
Experiment: Basic blocking



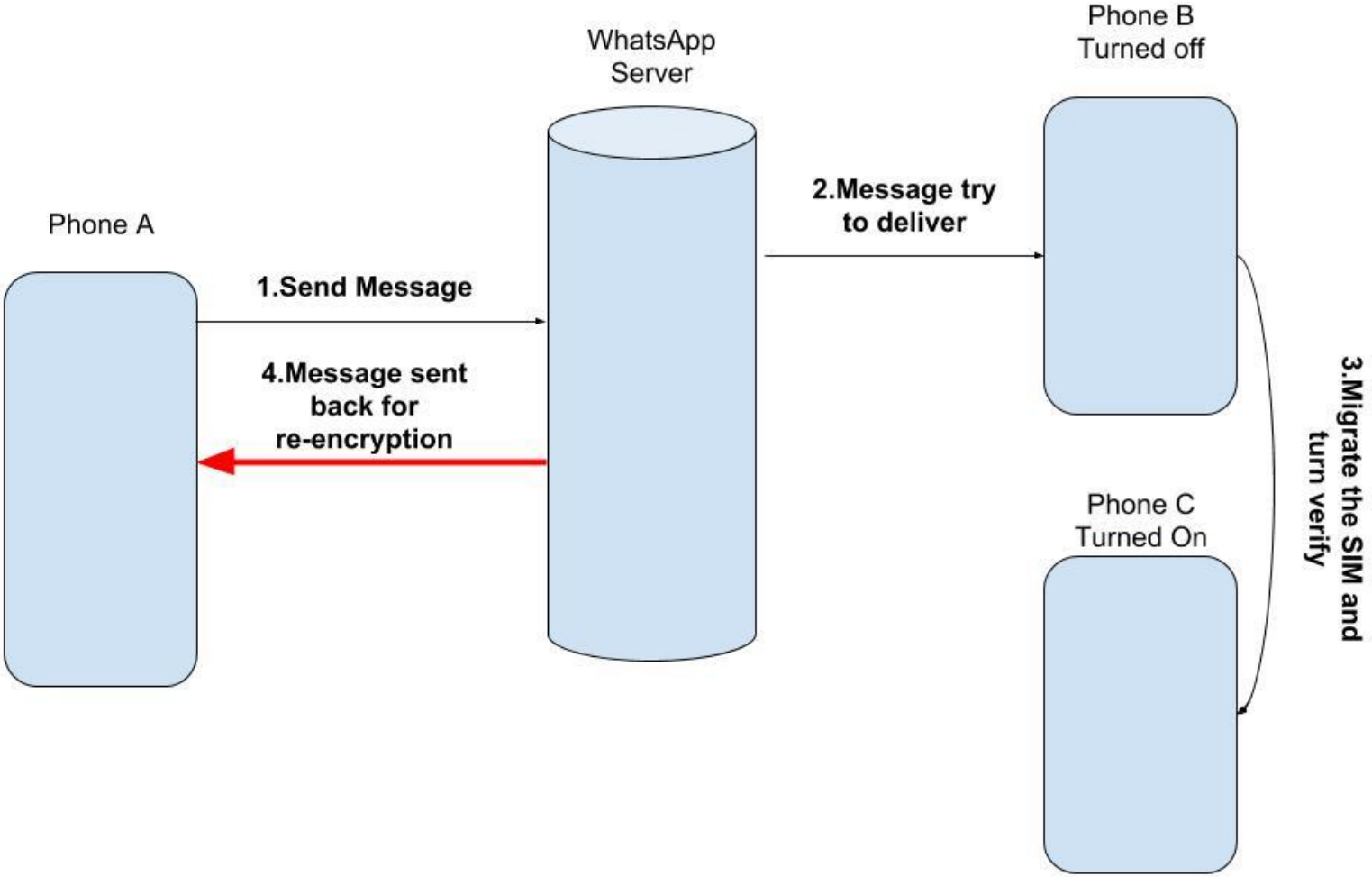
Experiment: Basic blocking



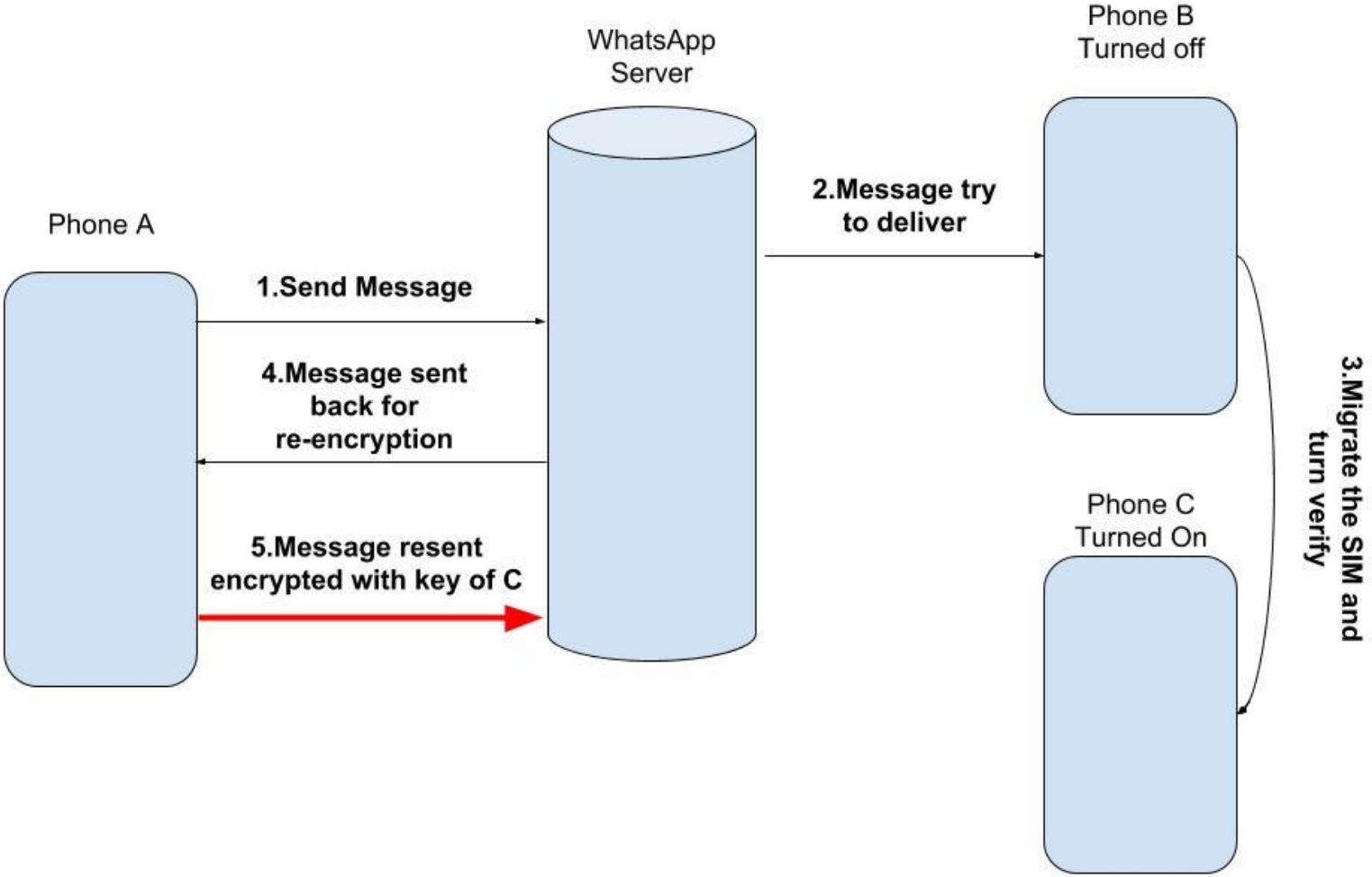
Experiment: Basic blocking



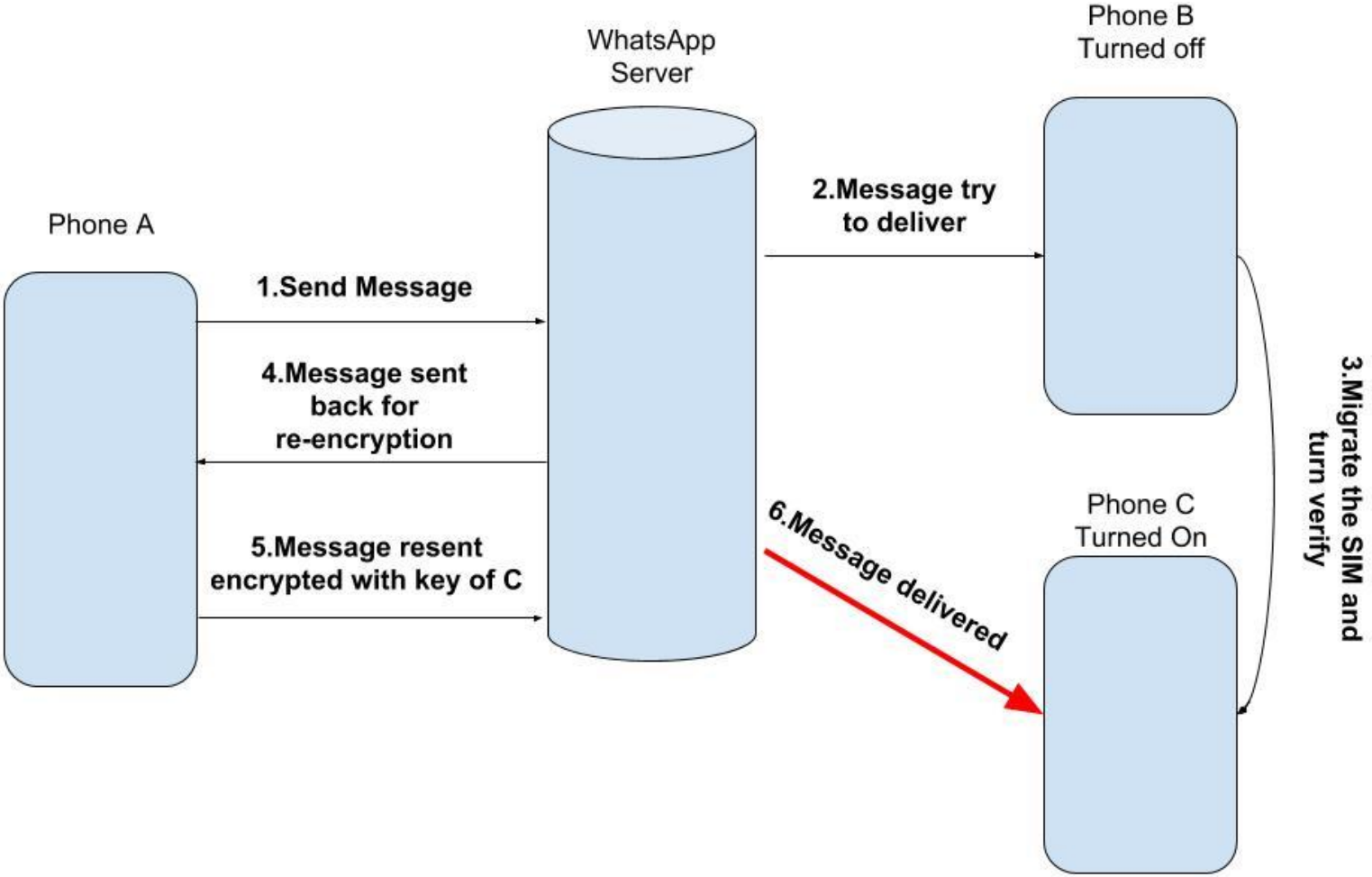
Experiment: Basic blocking



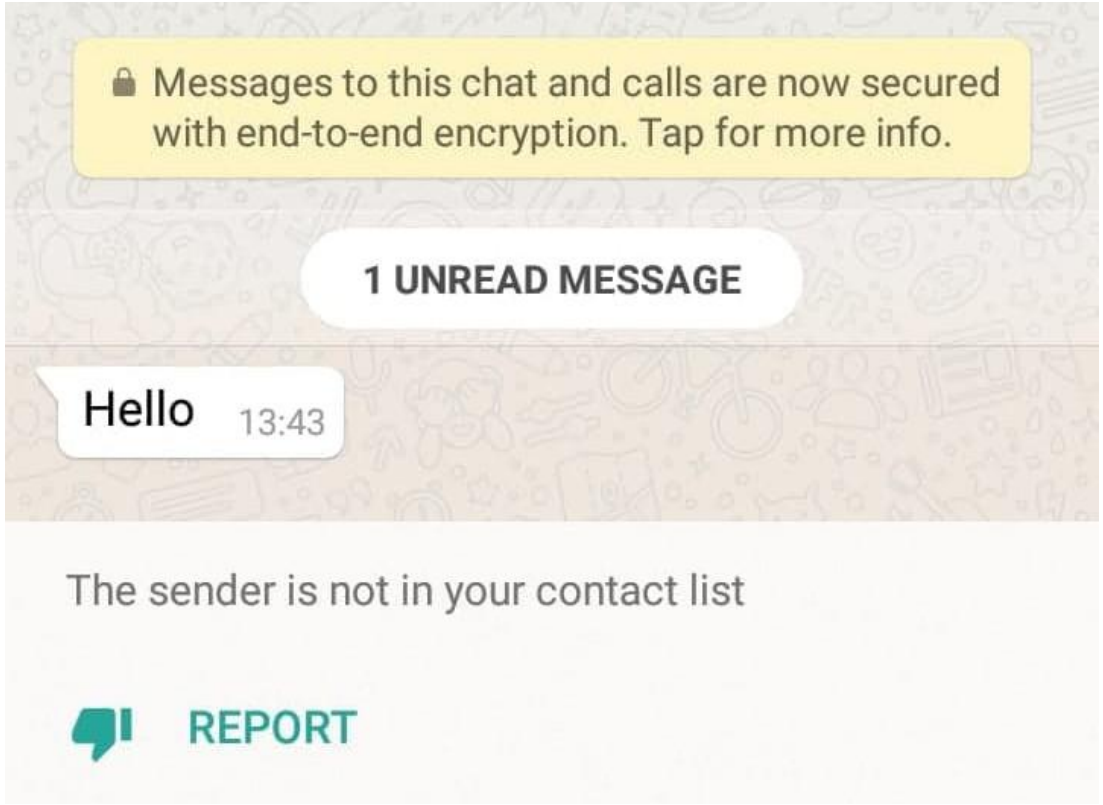
Experiment: Basic blocking



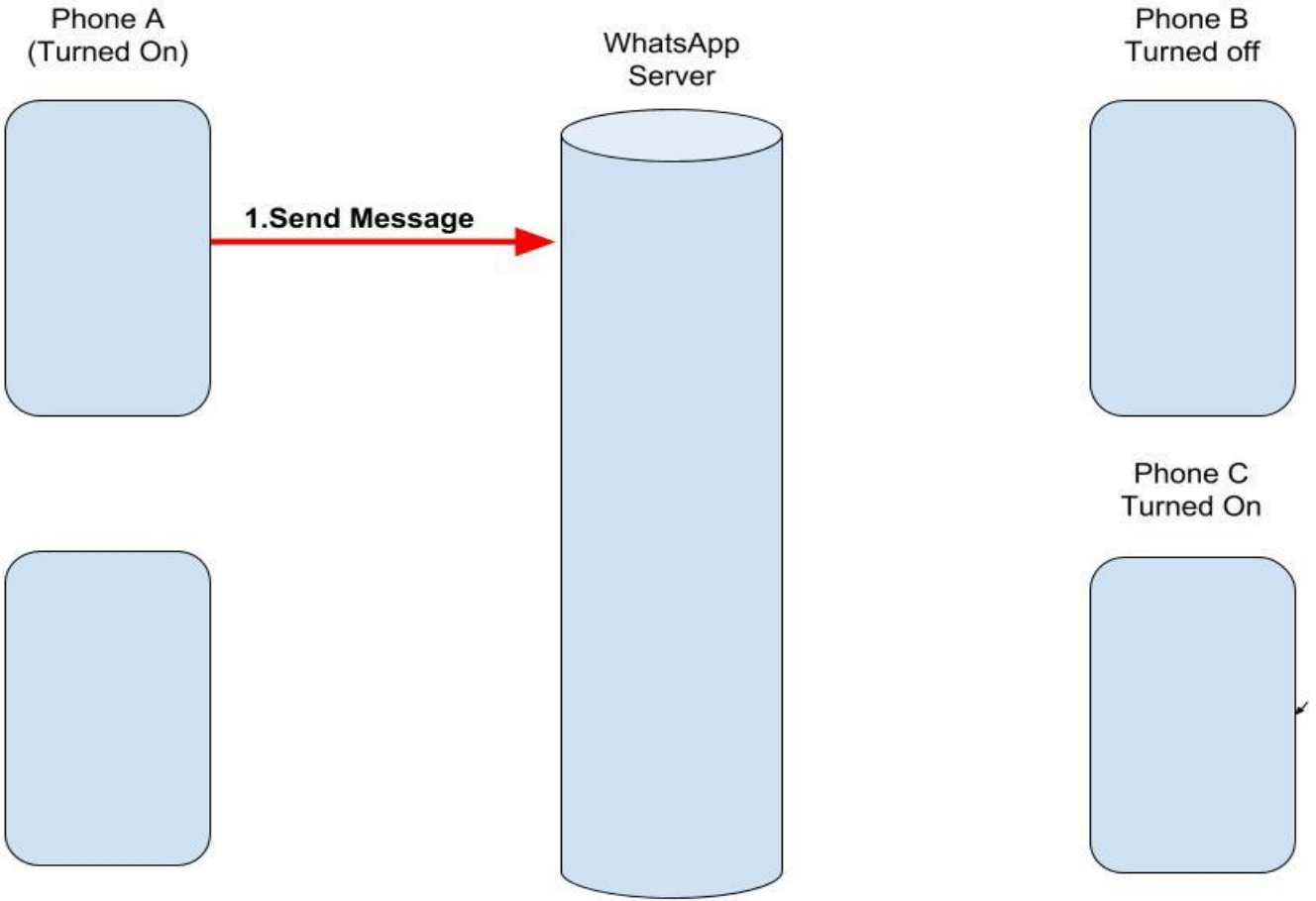
Experiment: Basic blocking



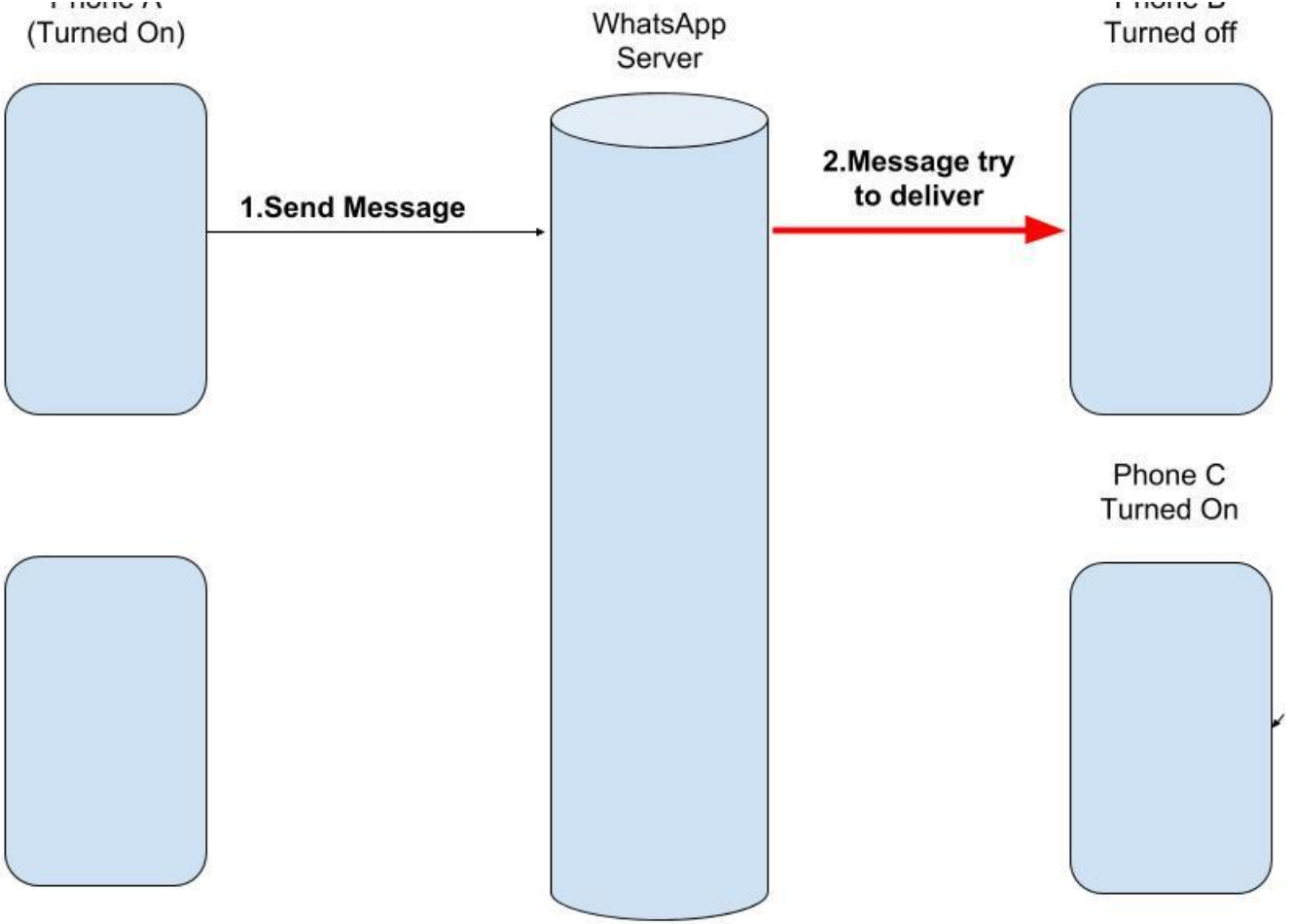
Results: Basic blocking



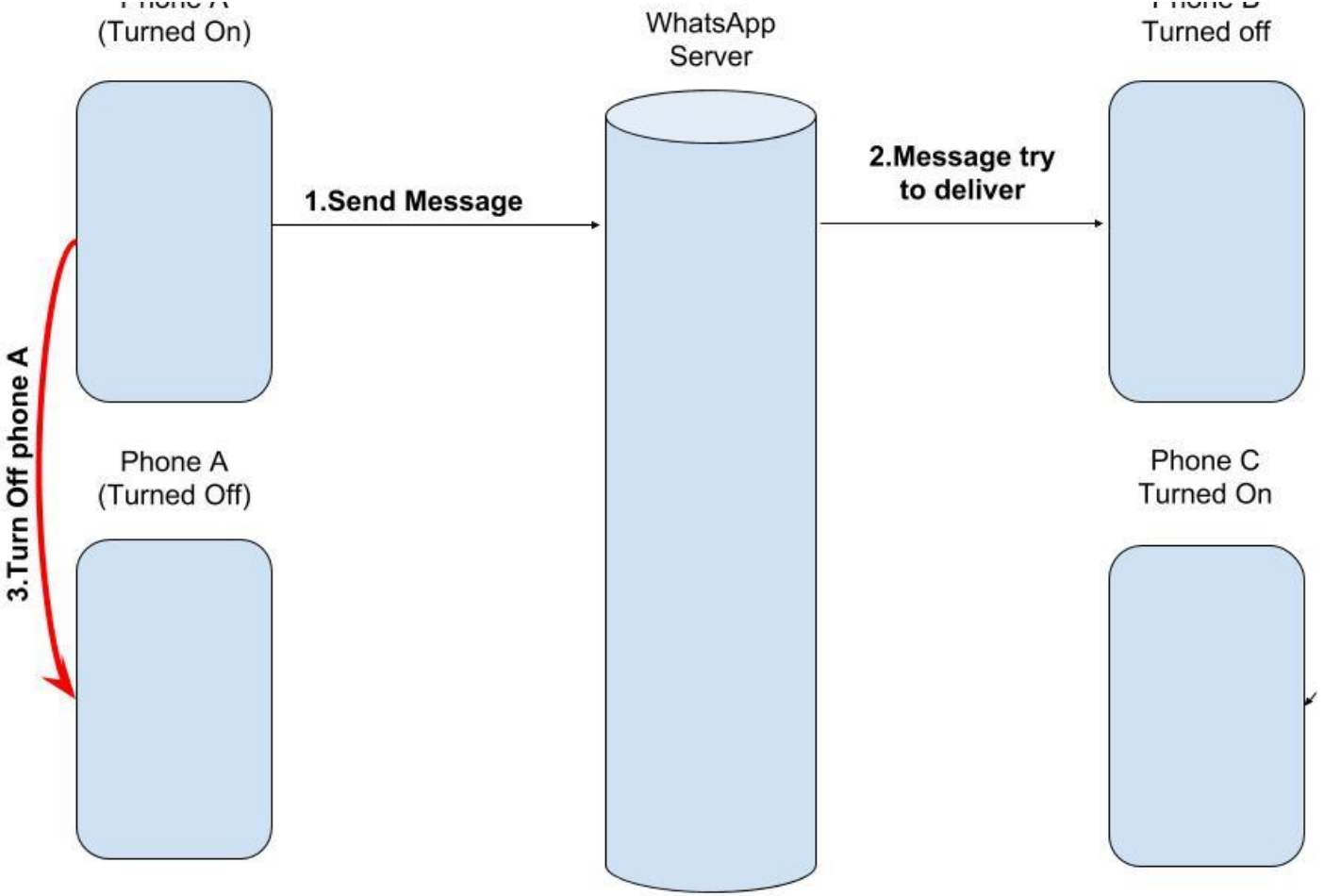
Experiment:Sender offline blocking



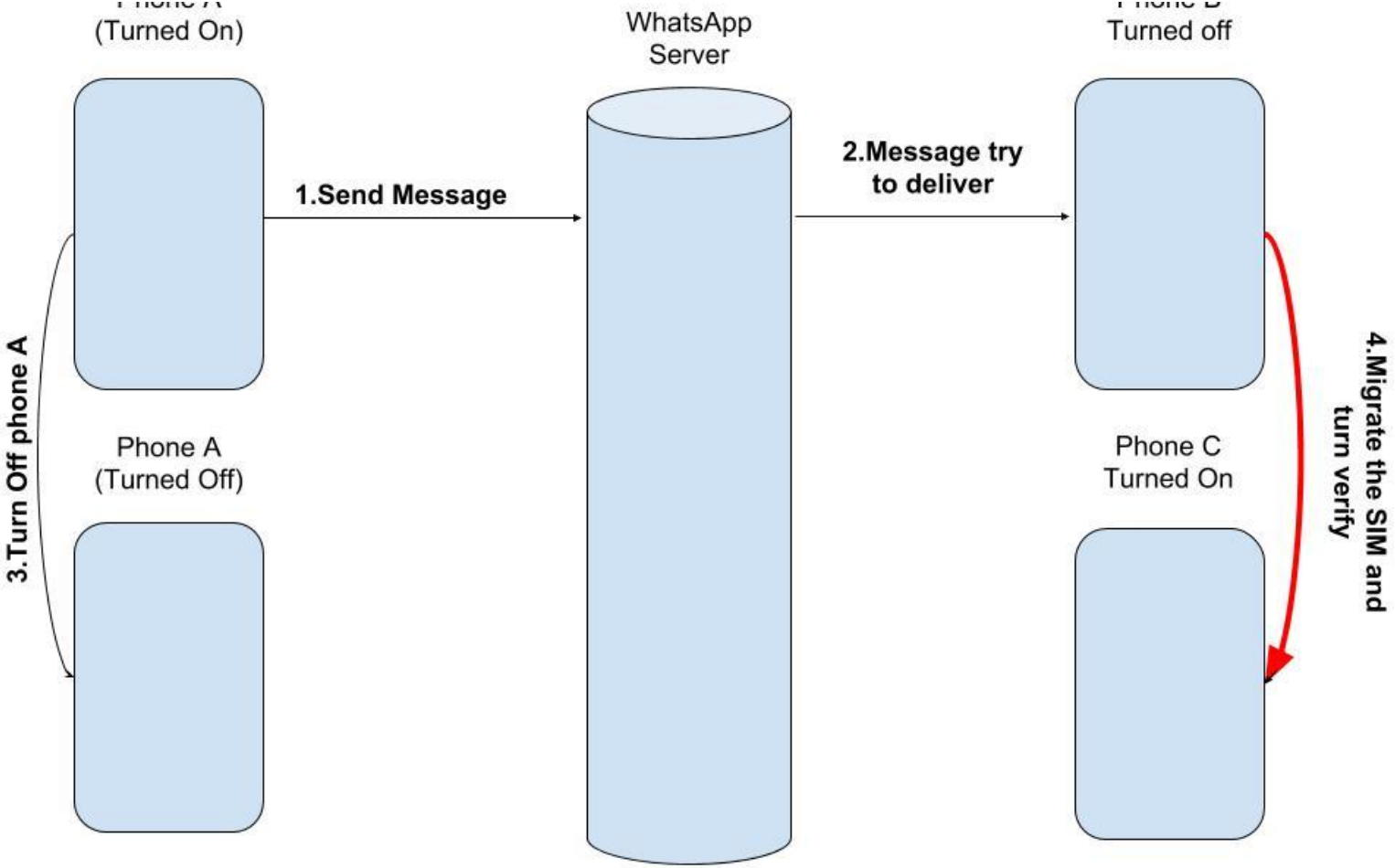
Experiment:Sender offline blocking



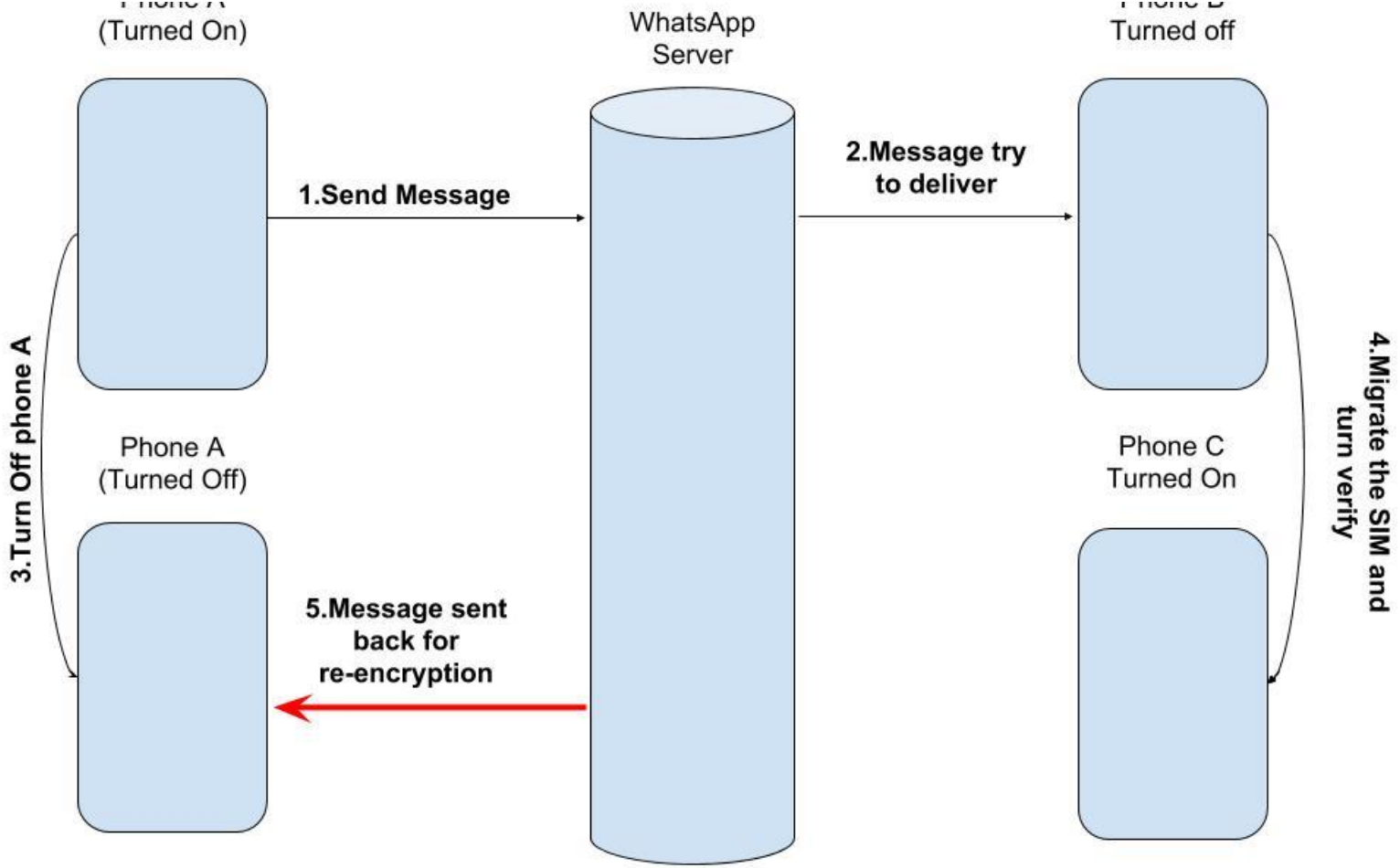
Experiment:Sender offline blocking



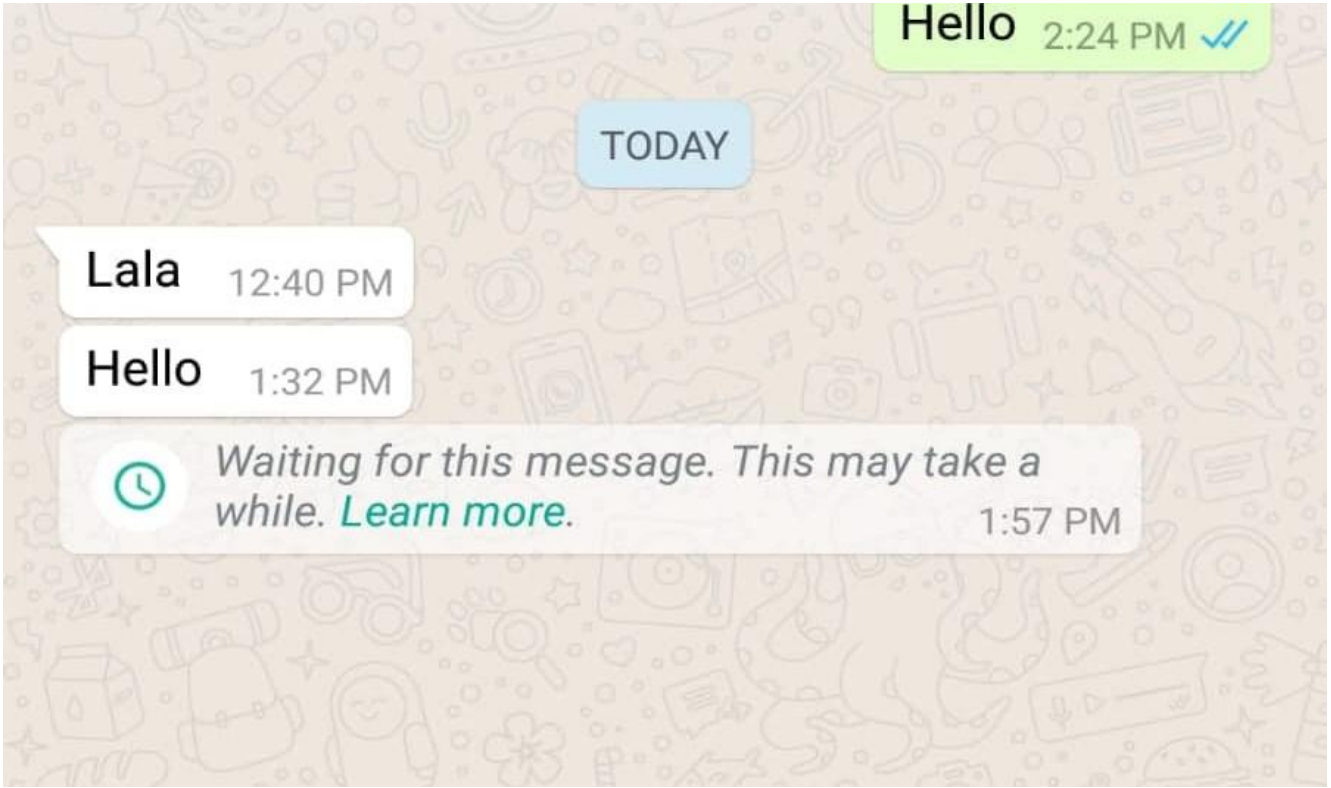
Experiment:Sender offline blocking



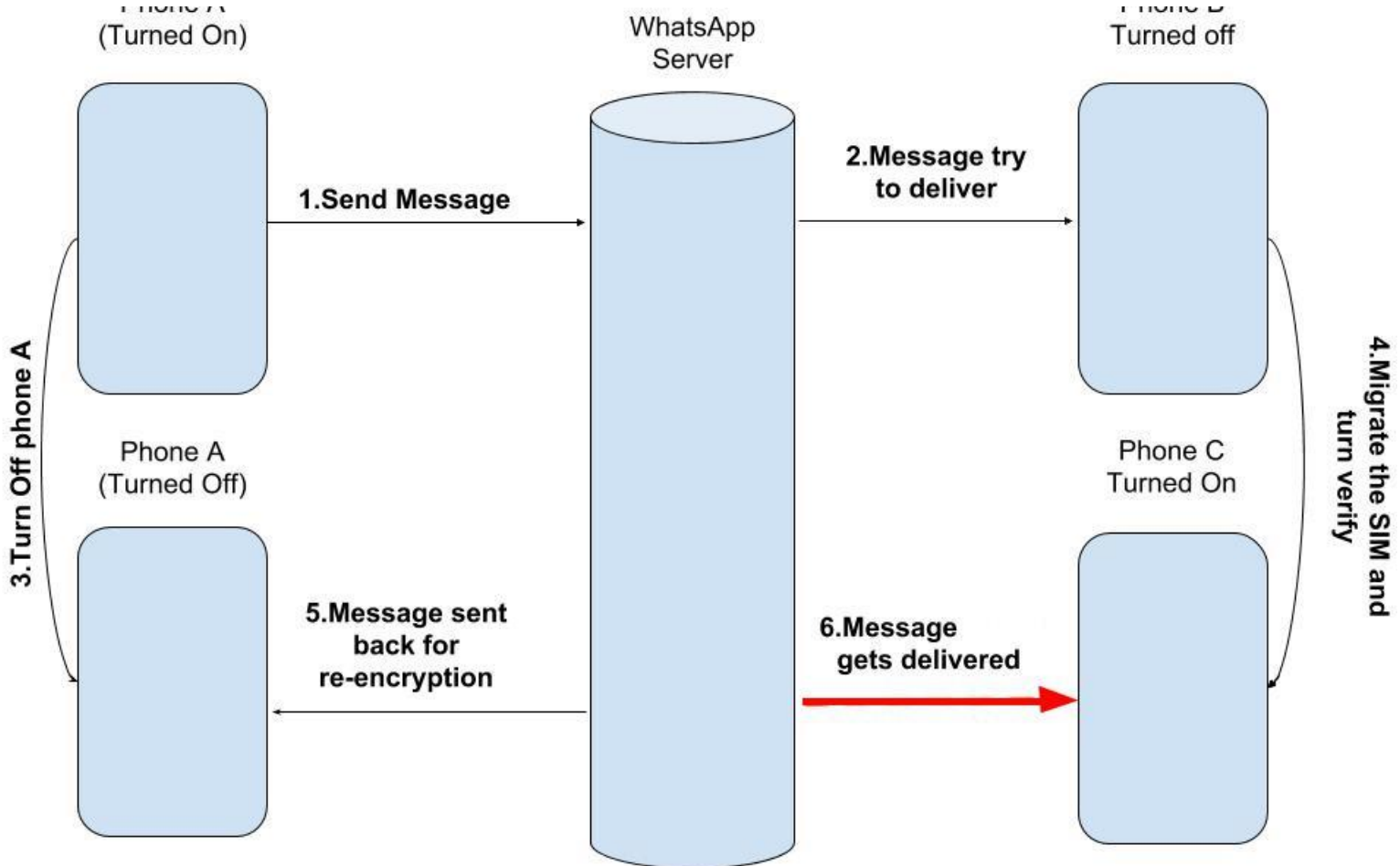
Experiment:Sender offline blocking



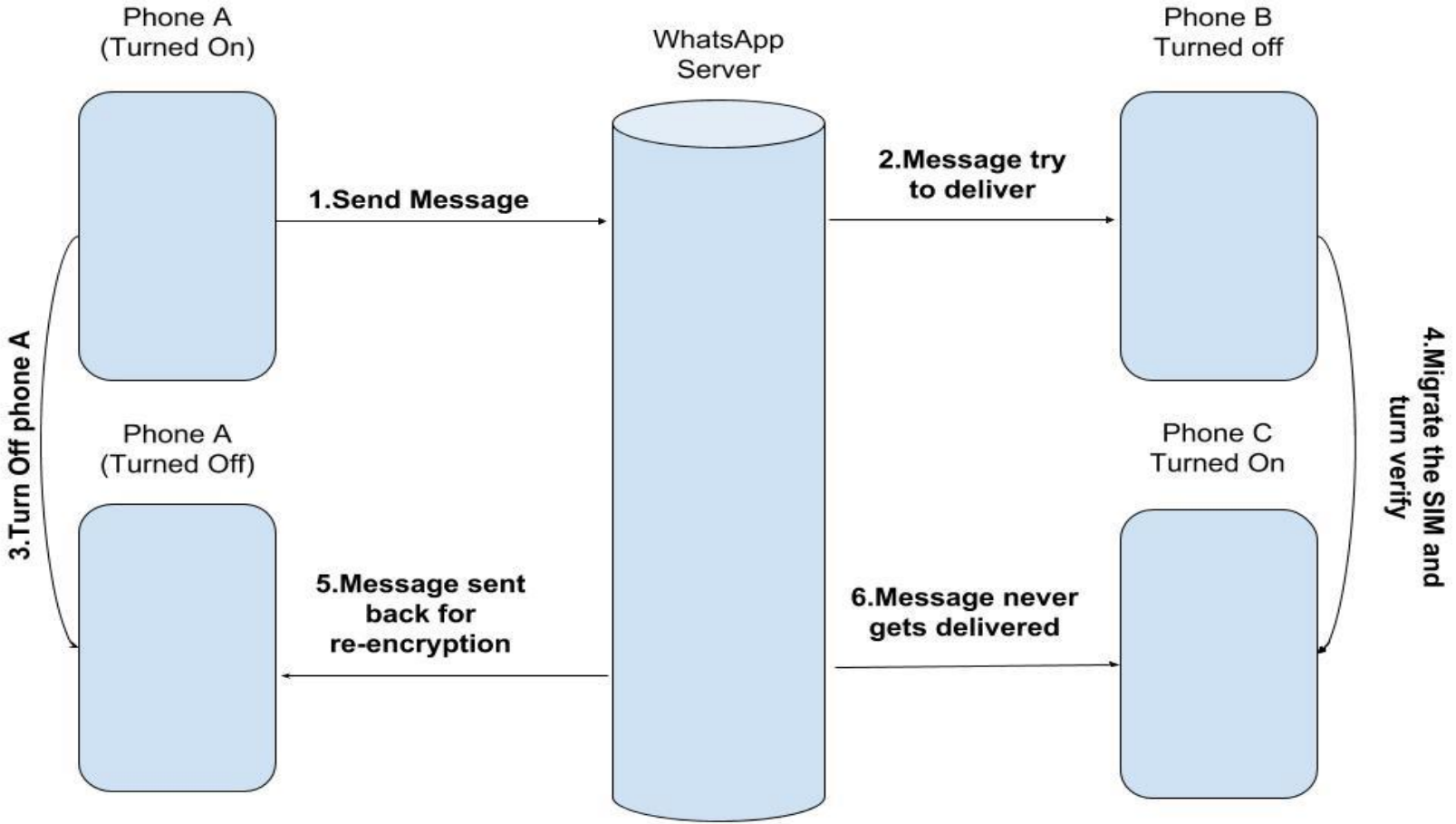
Results: Sender offline blocking



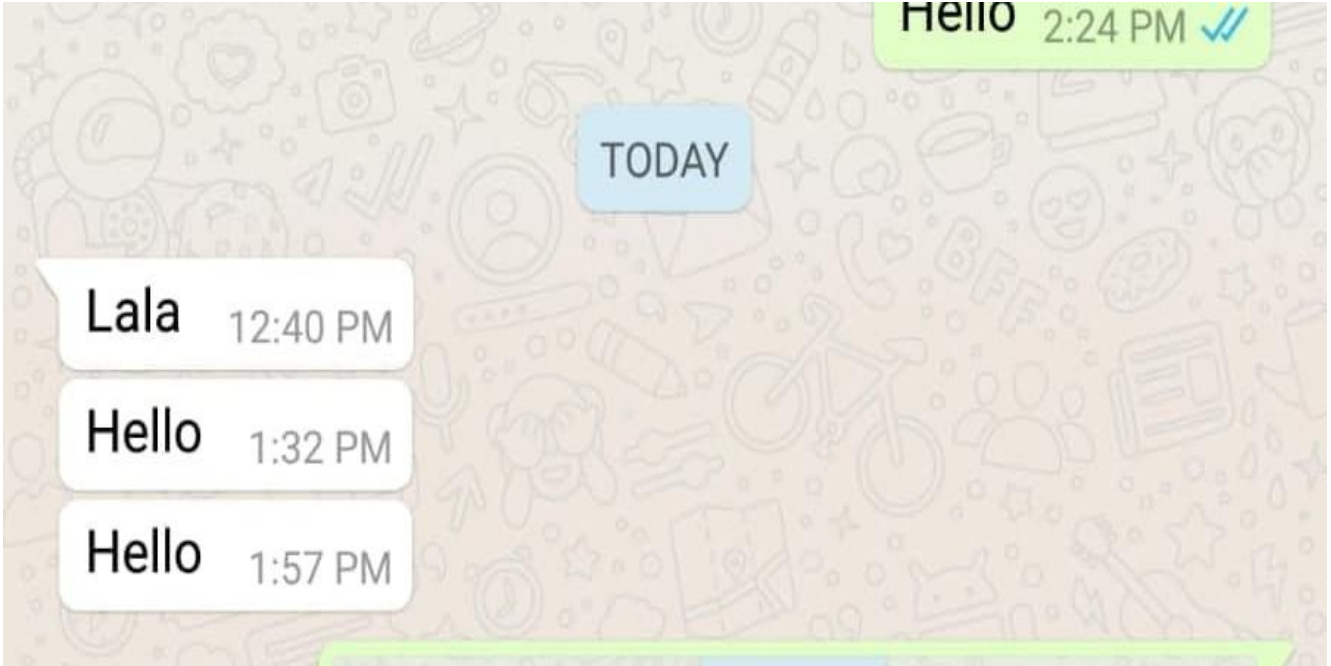
Experiment:Sender offline blocking



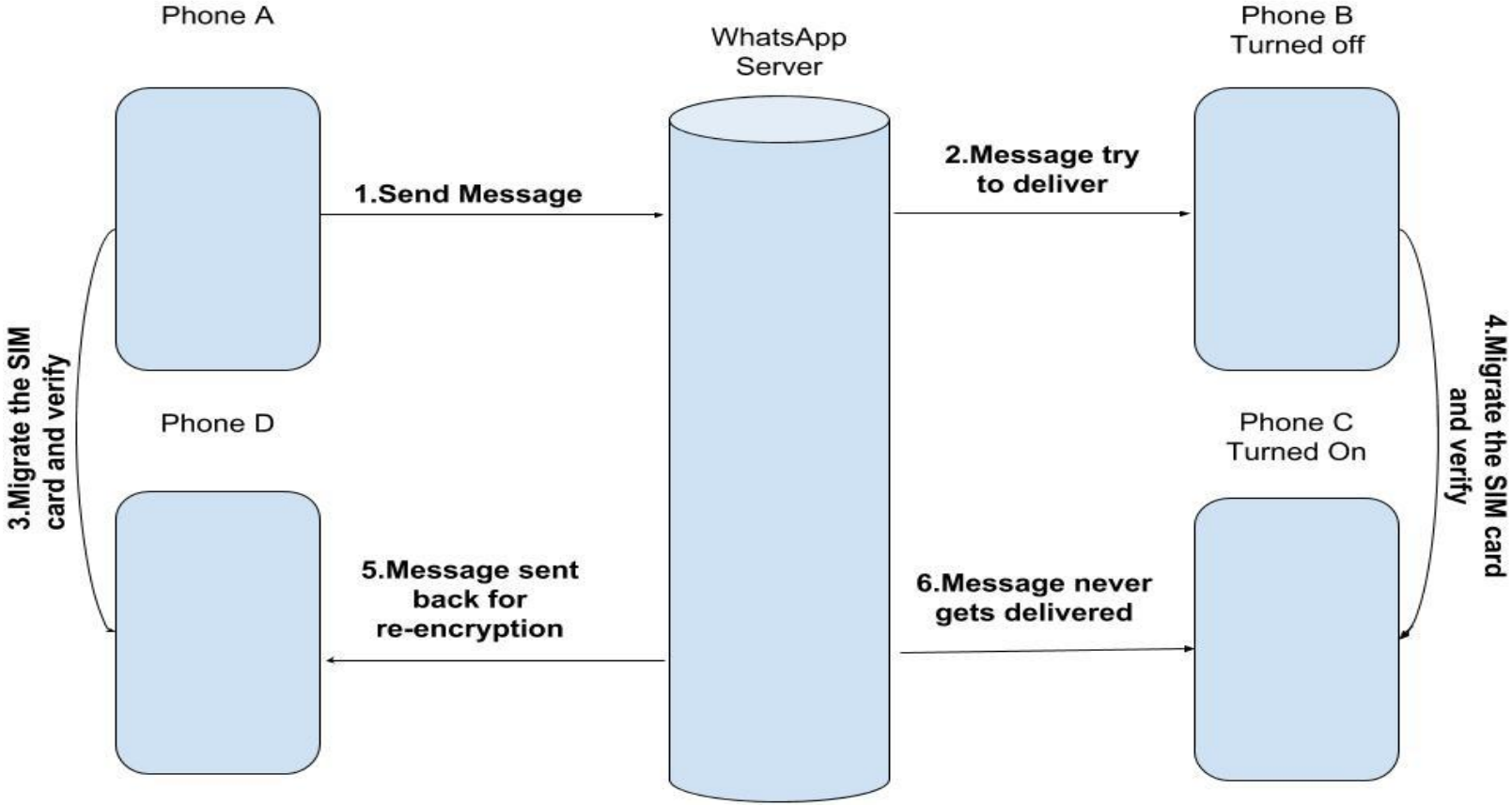
Experiment: Sender offline blocking



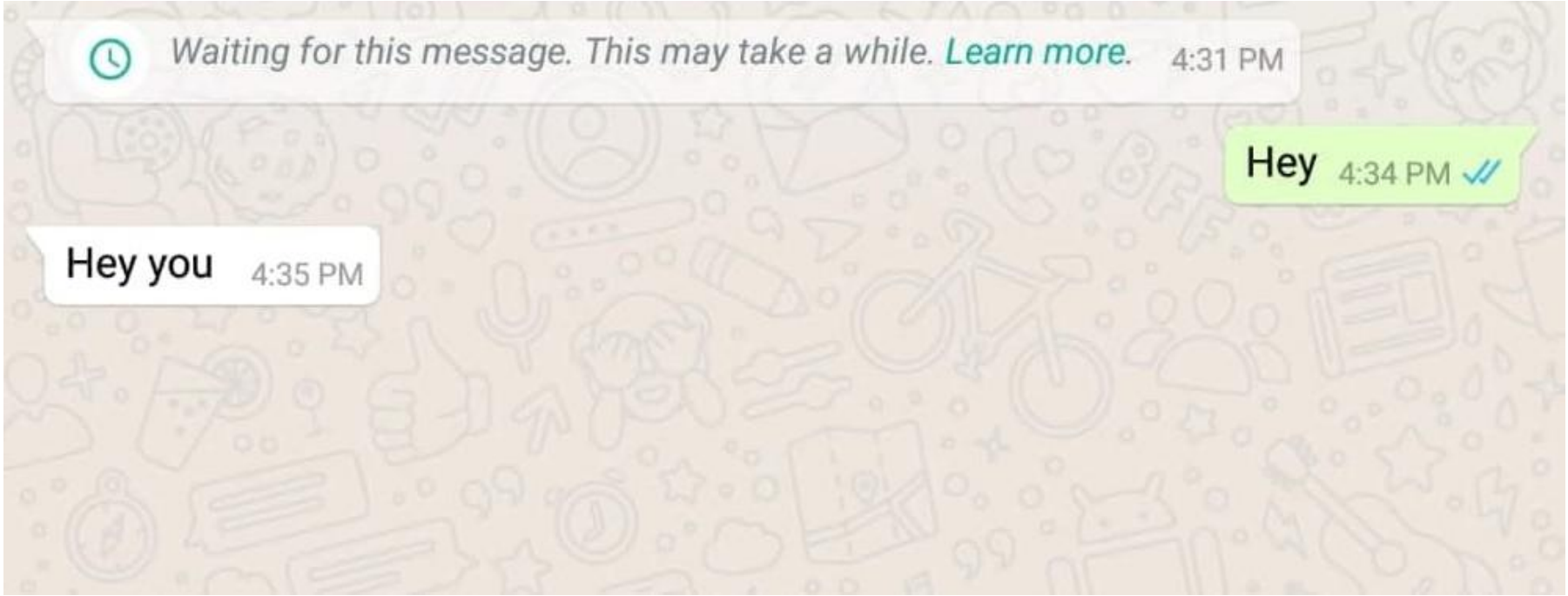
Results: Sender offline blocking



Experiment: Sender migration blocking



Results: Sender migration blocking



Discussion

- We expected the traffic of both applications to be more similar
- Decryption could verify the correct use of the Signal protocol

Future work

- Key extraction and message decryption (reverse engineering)
- Phone call verification abuse
- Metadata collection
- WhatsApp, Instagram and Messenger integration

Conclusion

- What are the algorithms used to create the Signal protocol?
- What are the differences between Signal and WhatsApp network traffic?
- To what extent are WhatsApp messages encrypted to the Signal protocol specifications?

Is user-to-user message exchange via WhatsApp end-to-end encrypted? *Probably yes*

References

- **[1]** P. R¨osler, C. Mainka, and J. Schwenk, “More is less: On the end-to-end security of group chats in signal, whatsapp, and threema,” 2018.
- **[2]** M. Marlinspike, “ There is no WhatsApp ’backdoor’),” 2017, last accessed 22 January 2019. [Online]. Available: https://signal.org/blog/there-is-no-whatsapp-backdoor/
- **[3]** M. Vigo, “Compromising online accounts by cracking voicemail systems),” 2018, last accessed 21 January 2019. [Online]. Available: https://www.martinvigo.com/voicemailcracker/
- **[4]** K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, “A formal security analysis of the signal messaging protocol,” in Security and Privacy (EuroS&P), 2017 IEEE European Symposium on. IEEE, 2017, pp. 451–466.
- **[5]** WhatsApp, “Whatsapp encryption overview,” April 5, 2016, p. 12.