Towards Next Generation Robust Cryptosystems

Deepak Puthal Newcastle University
Srinibas Swain IIIT Guwahati
Saraju P. Mohanty University of North Texas

***Abstract*—One of the key research directions aligning with the current and emerging consumer technology is cybersecurity. A variety of technologies including Internet-of-Things (IoT), IoT-Edge/Fog Computing, and embedded systems are gaining more importance in designing smart applications (e.g. smart cities, smart villages, and smart healthcare) with minimal human interventions. All the devices and datacentres in these applications are connected to the Internet for easy and smooth data transmission. Considering the Internet and communication medium properties, attackers get an easy chance to become part of the system and participate in the data communication process. This article presents thoughts on paradigm shift next generation cryptosystems to overcome the vulnerabilities of the omnipresent conventional cryptosystems.**

Vulnerability of Conventional Cryptosystem

Attackers are big threats to any system to let it not meet the purpose of the system deployment. The cryptosystems are designed to secure the data against potential attack patterns, such as attacks on integrity, and confidentiality. The existing cryptosystems can be broadly divided into two classes, i.e., Asymmetric Cryptography and Symmetric Cryptography [1]. Symmetric cryptography is a widely used cryptosystem to secure the data on the fly, and it is scalable with the resource constraint and tiny devices [1]. Asymmetric cryptography is considerably more secure, whereas it is 1000 times slower than symmetric cryptography [2]. This is normally use during the symmetric initial key transmission. The security level of the symmetric cryptosystem has become a primary concern to secure the system.

The conventional symmetric cryptosystem is based on the number theory games, where attackers are also aware of the operations of the encryption processes (see Figure 1). Improvising the number theory-based cryptosystem is not enough, because most of the time, attackers are equipped with high-performance computing infrastructure. The security of the cryptosystem is heavily dependent on the length of the encryption key. These fundamental drawbacks demand a novel way of data representation and operations for encryption. This may lead to set the bar higher for an attacker to compromise the data in an end-to-end process.

Graph Theory based Cryptosystems - A Novel Approach

This article introduces a novel graph theory based cryptosystem. The simplified process of the model is as shown in Fig. 2, and the steps are as follows.

1) According to the standard process, the plaintext is first converted into the binary format and then divided into the packet size.
2) After receiving the binary bits of the packet, the packets are divided into blocks. If the final block is not complete, it will fill with random bits to ensure all the blocks are of the same size.
3) Next, arrange the block's bits into a matrix format. Only the upper triangle will fill with the block bits and some random bits to create an undirected graph.
4) Subsequently, a graph operation (we call as clique injection, defined in the following Section) will be done in the upper triangular matrix to generate the random matrix as a ciphertext.

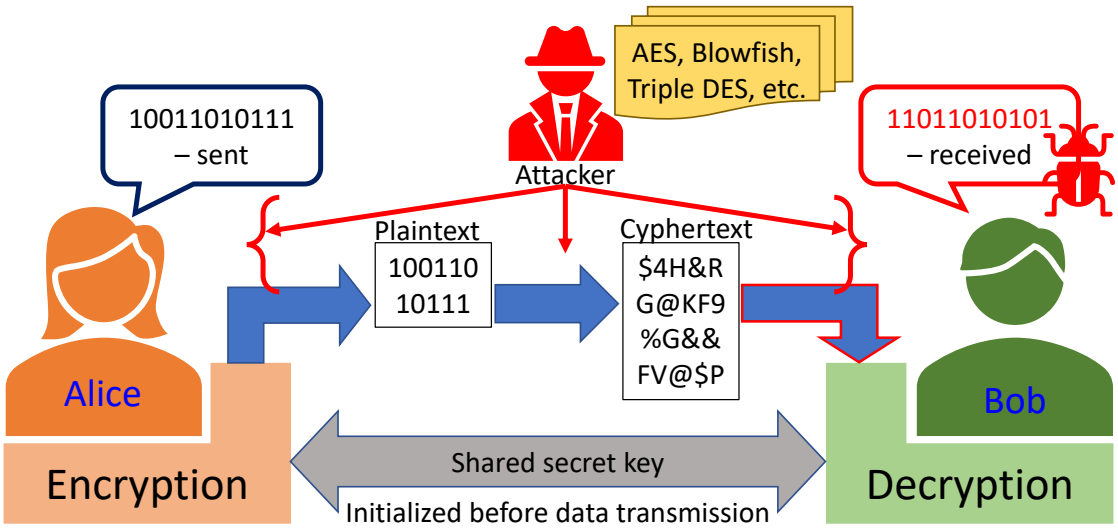

Fig. 1: Conventional Cryptosystem.

5) At the recipient end, inverse to the graph operation will be done to retrieve plain text from the ciphertext. The information required to complete the inverse function is used as the shared secret key.

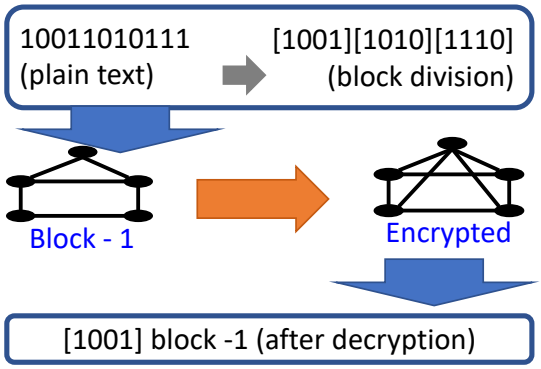

Fig. 2: Detailed process of graph Cryptosystem.

Graph Theory Based Cryptosystem - Robust Paradigm

We chose to use a graph theoretic encryption as it is simple yet combinatorially challenging. Graph theory is a field of mathematics, whose influence has far transcended the realm of mathematics. It has found a wide range of applications in all spheres of practical life. From finding an Euler tour in an intricate art gallery to solving the optimal layout in VLSI circuits, graph theory makes its presence felt [3]. A simple graph G may be defined as an ordered pair (V, E), where V is the vertex set, and $E \subseteq \{\{u, v\} : u, v \in V \wedge u \neq v\}$. The size of the vertex set is known as the order of the graph. Two vertices $v, w \in V$ are called adjacent if $\{v, w\} \in E$. A clique is a subset C of V such that every vertex in C is adjacent to every other; the clique number $\omega(G)$ of G is the size of the largest possible clique in G.

Finding a clique of order $k \geq 3$ in a graph G is an intractable problem. From a computational complexity stance, intractable problems are problems for which there exist no efficient algorithms (polynomial time algorithms with respect to the size of the input) to solve them. An enumeration version of this problem is "how many cliques of order $k \geq 3$ are there in a graph G?". In computational complexity theory the set of all enumeration problems is known as $\#P$ problems (refer Fig. 3).

In the aforementioned graph theoretic encryption if an intruder wants to decrypt the message without a valid key, the hacker either have to flip every bit of the encrypted message or has to enumerate all cliques of all orders in the encrypted graph. Both these methods take exponential time, whereas if the receiver has a valid key then the decryption of the encrypted message can be done in linear time.

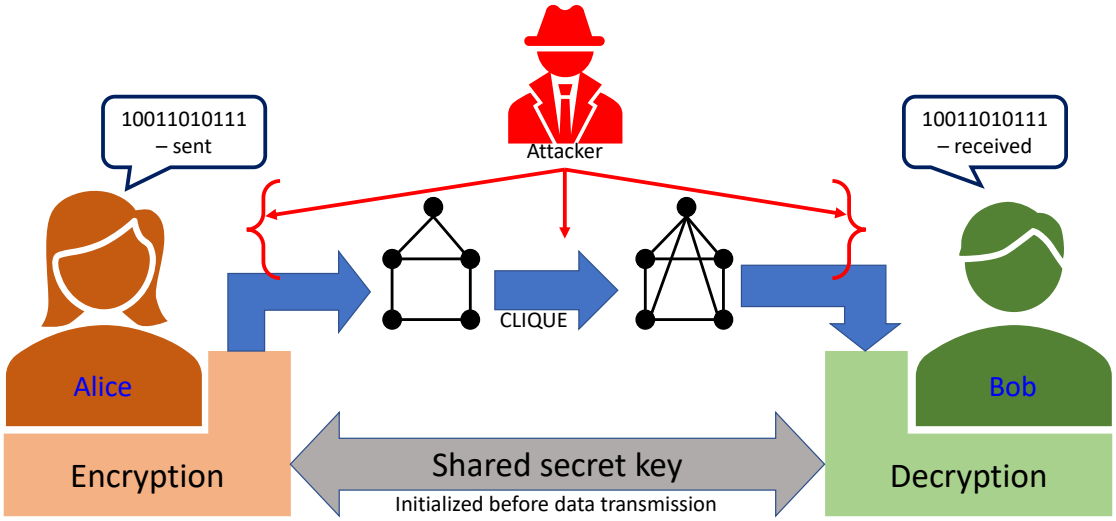

Fig. 3: Graph Theory based Cryptosystem.

Applications of Proposed Robust Cryptosystem - An Illustration

Unlike conventional symmetric cryptosystem, this model could be used in various domains, including the IoT-cloud, IoT-edge/fog computing, vehicular technology, and healthcare technology [4], [5], [6]. This model will reduce the chances of possible network attacks by increasing complexity for the attackers. Therefore, data communication over an insecure network will be relatively secure than the current approach. The smart applications, such as smart cities/villages and smart healthcare, will be secure and scalable by meeting the purpose of deployment with our new cryptosystems.

Conclusion and Future Directions

Introducing graph theory and clique injection will set the bar higher for an attacker to break the cryptosystem and extract the original plaintext.

In the future, this cryptosystem should deploy and experiment in both simulation and testbed environments to validate by designing possible network threat models.

References

[1] D. R. Stinson and M. Paterson, *Cryptography: theory and practice*. CRC press, 2018.

[2] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "DLSeF: A dynamic key-length-based efficient real-time security verification model for big data stream," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 2, pp. 1–24, 2016.

[3] J. A. Bondy, U. S. R. Murty *et al.*, *Graph theory with applications*. Macmillan London, 1976, vol. 290.

[4] D. Puthal, S. P. Mohanty, S. Wilson, and U. Choppali, "Collaborative edge computing for smart villages," *IEEE Consumer Electronics Magazine*, no. 10.1109/MCE.2021.3051813, 2021.

[5] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, 2019.

[6] V. K. Kukkala, J. Tunnell, S. Pasricha, and T. Bradley, "Advanced driver-assistance systems: A path toward autonomous vehicles," *IEEE Consumer Electronics Magazine*, vol. 7, no. 5, pp. 18–25, 2018.

Deepak Puthal is Assistant Professor at the School of Computing, Newcastle University, Newcastle upon Tyne, UK. Contact him at: deepak.puthal@newcastle.ac.uk.

Srinibas Swain is an assistant professor at the Department of Computer Science and Engineering, IIIT Guwahati, India. Contact him at: srinibas@iiitg.ac.in.

Saraju P. Mohanty is a Professor in the Department of Computer Science and Engineering, University of North Texas, Denton, USA. Contact him at: smohanty@ieee.org.