Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Efficient SDRP with Elliptic Curve Integrated Encryption Scheme

Ruchika Markan, Gurvinder Kaur

Assistant Profssor[1]

Department of Computer Science

RIMT-Institute of Engineering and Technology

Mandi Gobindgarh, India

Abstract: ***Wireless reprogramming in a wireless sensor network (WSN) is the process of propagating a new code image or relevant commands to sensor nodes. As a WSN is usually deployed in hostile environments, so for security reasons every code update must be authenticated to prevent an adversary from installing malicious code in the network. The reprogramming protocols based on the distributed reprogramming approach allow multiple authorized network users to simultaneously and directly reprogram sensor nodes without involving the base station. SDRP is the first distributed reprogramming protocol. In this research Elliptic Curve Integrated Encryption Scheme is used for providing strong security to sensor network. Only authorized users will be allowed to update the system reprogramming and with according to privileges carried by user, system upgrade options will be provided. User privilege and identity will be checked with signature of the message. For managing privacy preservation between owner and other user's different session keys for owner and users are introduced so that both can have different views of network and can also preserve their privacy from each other.***

Keywords: ***Sensor Networks, Network Reprogramming, Distributed, Authentication***

I. INTRODUCTION

Wireless sensor networks may be deployed for long periods of time during which the requirements from the network owner and users or the environment in which the nodes are deployed may change[19]. The change may necessitate uploading a new code image or retasking the existing code with different sets of parameters. We refer to both of these activities as reprogramming. One of the proclaimed advantages of sensor networks is their ability to operate for extended periods of time without physical intervention by humans. For example, sensor networks may be used in remote or hostile locations too dangerous for humans to enter. In environmental applications, sensor networks can be used where the mere presence of humans during the study may disturb results. The very nature of these applications makes physical interaction with nodes for maintenance purposes unacceptable. Nevertheless, users must be able to add or change the functionality of a deployed network to fully utilize its capabilities. It is clear that network reprogramming is required for the success of wireless sensor networks. In many cases, complete knowledge of an environment is not known and makes predicting what actions to perform and when to perform them a difficult, if not impossible, task when developing a sensor network application. Additionally, requirements and environments may evolve over time, making the ability to add or change functionality of a deployed network imperative. Developers face a more immediate problem. As sensor network research matures, the number of nodes used in test beds and deployments continues to grow. To support network reprogramming, protocols for the reliable distribution of a program image to nodes are required.

While wireless sensor networks have attracted increasing research attention, protocols designed for wireless sensor networks have generally focused on the processing and communication of relatively small data objects, though not without reason. In general, data generated by individual nodes, such as temperature values, usually have representation sizes on the order of bytes. Additionally, the resource limitations of nodes have encouraged greater focus on designing for small data objects. For example, the low bandwidth of the radio has kept communication packets small with a typical size around tens of bytes. Small packets, combined with limited memory and computation capabilities, have provided little reason to consider large data objects on the order of kilobytes.

II. REQUIREMENTS AND PROPERTIES OF PROGRAMMING PROTOCOLS

The reprogramming protocols, protocol should satisfy the following requirements.[1]

1) **Authenticity** and **integrity of code images**: The source of a program image must be verified by a sensor node before installation, ensuring that only a trusted source can install a program. In addition, integrity means that an updated program image cannot be modified undetectably.

2) **Freshness**: An earlier version of a program image cannot be installed over the program with the same or greater version number, ensuring that a node always installs the newest version of a program image.

3) **Node compromise tolerance**: A compromised node must be prevented from causing an uncompromised node to violate the aforementioned security requirements. Other than meeting the aforementioned requirements, a reprogramming protocol should also have the following properties.

1) **Distributed**: The authorized network users are able to simultaneously and directly update code images on the nodes without involving the base station. At the same time, the protocol should prevent unauthorized users from updating sensor nodes.
2) **Supporting different user privileges**: To ensure smooth functioning for a WSN, the level of each user privilege should be limited by the network owner.
3) **Partial reprogram capability**: To prevent sensor nodes from being totally controlled by network users, the special modules on each sensor node cannot be overwritten by anyone except the network owner.
4) **User traceability**: In most application scenarios, traceability is highly desirable, particularly for reprogramming.
5) **Being efficient**: Mobile devices, particularly sensor nodes, usually have limited resources. Thus, energy efficiency (with respect to both communication and computation) and small storage overhead should be given priority to cope with the resource-constrained nature of WSNs.
6) **Scalability**: First, the protocol needs to be efficient even in a large-scale WSN with thousands of sensor nodes, and second, the protocol should be able to support a large number of users.

III. CLASSIFICATION OF REPROGRAMMING PROTOCOLS

Several reprogramming protocols have been proposed to propagate new code images in WSNs. The reprogramming protocols are based on the centralized approach in which only the base station has the authority to reprogram the sensor nodes. When the base station wants to disseminate a new code image to certain sensor nodes, it transmits the signed code image to those nodes via multihop routing, and those nodes only accept the code image signed by it. Unfortunately, the centralized approach is vulnerable to the single point of failure and not reliable because reprogramming becomes impossible when the base station fails or when some nodes lose connections to the base station. Also, it is inefficient, weakly scalable, and vulnerable to potential attacks along the long communication path . The base station has to be online and accessible to any user at any time during the network operation. Even worse, there are some WSNs that do not have any base station. Examples of such networks include a WSN deployed along an international border to monitor weapon smuggling and human trafficking. Having a base station in these WSNs introduces a very attractive attack target. Obviously, for such networks, it is necessary to have authorized network users to be able to carry out reprogramming in a distributed manner. Distributed reprogramming approach is that, in which multiple authorized users are supported, each user may have a different privilege of reprogramming sensor nodes. This is particularly important in large-scale sensor networks owned by an owner and used by different users from both public and private sectors.

IV. PERFORMANCE MATRICES FOR SDRP

1) Delay

The packet delay is the time of creation of a packet by the source node up to the destination node reception. At this time a packet starts to move across the working network. Time usually expressed in seconds. Hence all the delays in the network are called packet end-to-end delay, like buffer queues and transmission time. This delay can be called as latency; it provides same sense as delay. There are different kinds of activities because of which network delay is increased. Packet end-to-end delay is a measure of how sound a routing protocol adapts to the various constraints in the network to give reliability in the routing protocol [16]. We have several kinds of delays which are processing delay (PD), queuing delay (QD), transmission delay (TD) and propagation delay (PD). The queuing delay (QD) is not included, as the network delay has no concern with it [16].

2) Throughput

Throughput is defined as the ratio of the total data reaches a receiver from the sender [15]. Throughput is expressed as bytes or bits per sec (byte/sec or bit/sec). Some factors affect the throughput as; if there are many topology changes in the network, unreliable communication between nodes, limited bandwidth available and limited energy. A high throughput is absolute choice in every network.

3) Upload response time

Upload response time is the time taken for a page to upload per second. It is very essential parameters to consider if we are going with authentication and secure communication

V. SDRP Protocol

SDRP [1] is the first protocol which supports distributed reprogramming. While all existing insecure/secure reprogramming protocols are based on the centralized approach, it is important to support distributed reprogramming in which multiple authorized network users can simultaneously and directly reprogram sensor nodes without involving the base station. Very recently, a novel secures and distributed reprogramming protocol named SDRP was proposed, which is the first work of its kind.
SDRP consists of three phases: system initialization, user preprocessing, and sensor node verification. In the system initialization phase, the network owner creates its public and private keys and then assigns the reprogramming privilege and the corresponding private key to the authorized user(s). Only the system public parameters from the network owner are loaded on each sensor node before deployment. In the user preprocessing phase, if a network user enters the WSN and has a new program image, he will need to construct the reprogramming packets and then send them to the sensor nodes. In the sensor node verification phase, if the packet verification passes, then the nodes accept the program image.

VI. Elliptic Curve Integrated Encryption Scheme (ECIES)

Integrated Encryption Scheme (IES) is a hybrid encryption scheme which provides semantic security against an adversary who is allowed to use chosen-plaintext and chosen-cipher text attacks. The security of the scheme is based on the problem. The elliptic curve integrated encryption system (ECIES) is the standard elliptic curve based on encryption algorithm. It is called integrated, since it is a hybrid scheme that uses a public key system to transport a session key for use by a symmetric cipher. ECIES is a public-key encryption algorithm. [3]

To send an encrypted message to Bob using ECIES Alice needs the following information:

- cryptographic suite to be used:
  - KDF
  - MAC
  - symmetric encryption scheme E
- EC domain parameters(p,a,b,G,n,h) for a curve over prime field or (m,f(x),a,b,G,n,h) for a curve over binary field;
- Bob's public key: K_B(Bob generates it as follows: $K_{B=} K_B G$, where K_B is the private key he chooses at random: K_B€ [1, n-1]
- optional shared information: S_1 and S_2.

To encrypt a message m Alice does the following:

1. generates a random number r € [1,n-1] and calculates R = rG;
2. derives a shared secret: S = P_x, where P = (P_x, P_y) = rK_B (and P ≠ 0)
3. uses KDF to derive a symmetric encryption and a MAC keys: K_E || K_M = KDF(S||S_1);
4. encrypts the message: c = E(K_E; m);
5. computes the tag of encrypted message and S_2: d = MAC(K_M; c||S_2); outputs R||c||d.

To decrypt the ciphertext R||c||d Bob does the following:

1. derives the shared secret: S = P_x , where P = (P_x, P_y) = K_BR (it is the same as the one Alice derived because P = K_BR = K_BrG = rK_BG =rK_B), or outputs *failed* if P = 0;
2. derives keys the same way as Alice did: K_E||K_M = KDF(S||S_1);
3. uses MAC to check the tag and outputs *failed* if d ≠ MAC(K_M ; c||S2);
4. uses symmetric encryption scheme to decrypt the message m = E^{-1}(K_E; c)

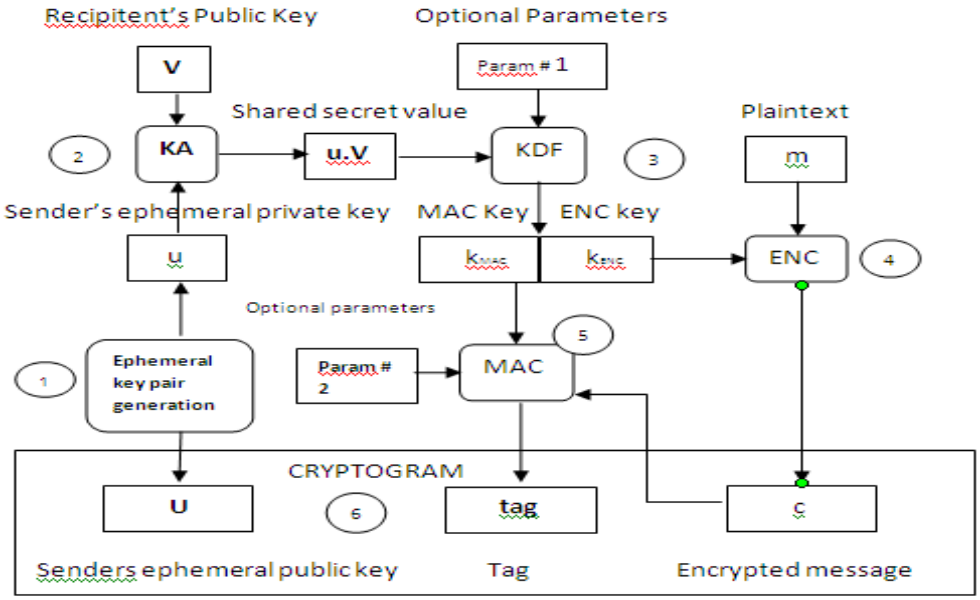


Fig. 1.1ECIES Encryption Functional Diagram

VII. IMPLEMENTATION AND PERFORMANCE EVALUATION

The main contributions of this paper are as follows:

Wireless sensor networks reprogramming process have many challenges including the unauthorized users. For these issues we have considered good solutions for it and some of the objectives which used to fulfill the required milestones in the research. First milestone in the research is providing concept of privacy preservation to users by implementing the clusters in sensor network with elliptic curve for more secure communication and authentication. The remaining milestone is to provide user authentication based attacks and prevention by implementing integrated elliptic curve.

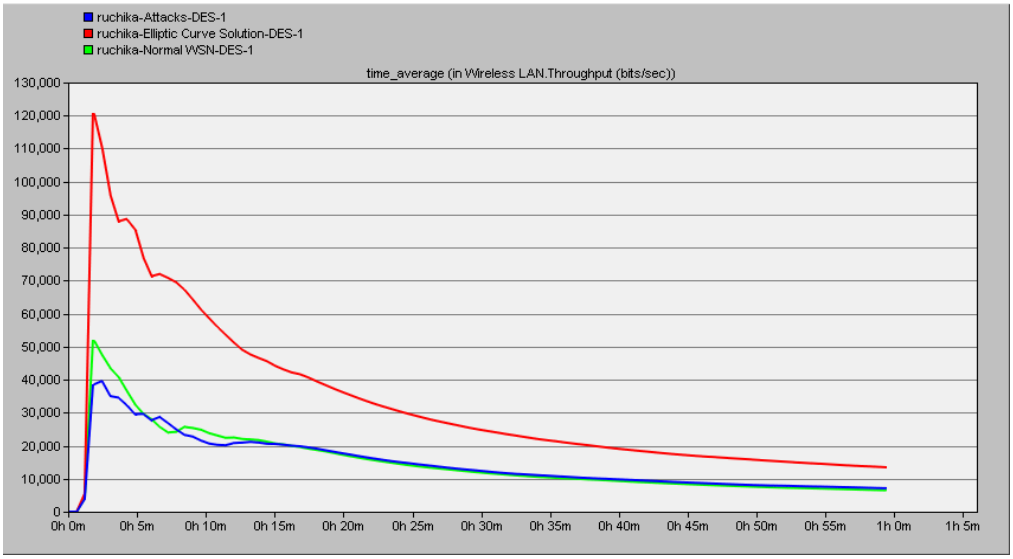
A. Implementation

The experimentation is started with briefing knowledge about sensor network and the basic implementation of sensor network in OPNET 14.5 Modeler Simulator. Sensor field will be used as logical area of 500 × 500 square with various

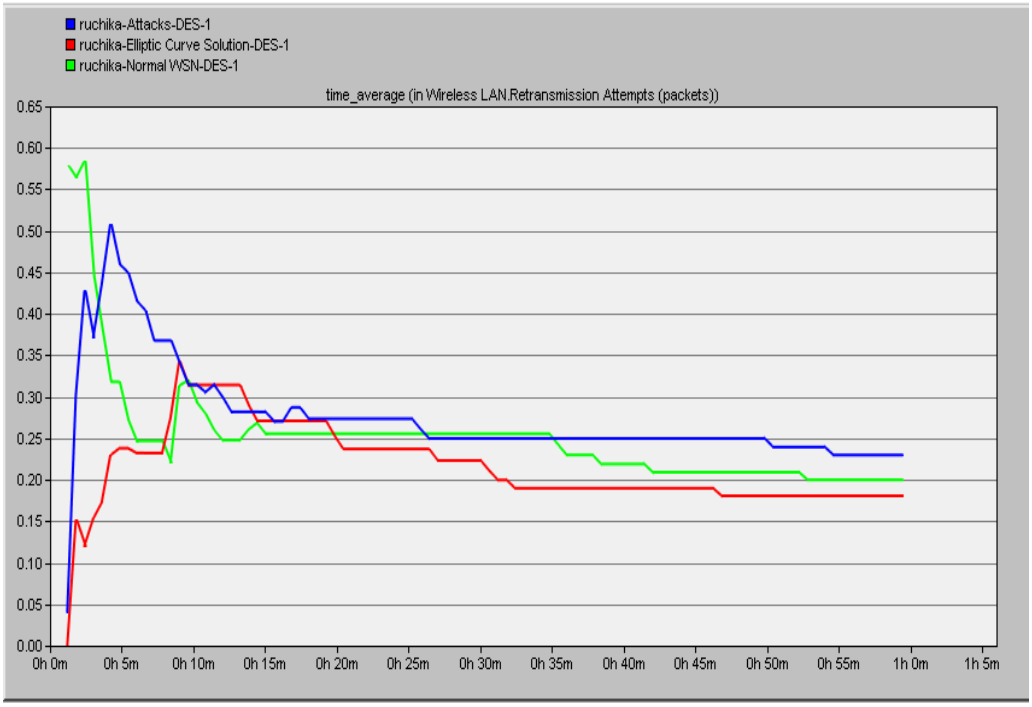
sensor nodes and Single sink. We start our proceeding with pre deployment of sensor nodes and continue with implementation of traffic on sensor network. After this process we will distribute the predefined asymmetric keys to all sensors. This key distribution will provide public encryption to the deployed network. Next step will be of selection of cluster head selection has been done on the bases of total energy depleted by the sensor. Sensor with more energy remaining will become the cluster head. Energy will also be measured and must be more than threshold energy level. Next step is to provide public key security to the sensor network. User will store the Elliptic Curve Integrated Encryption for providing strong security to sensor network. Only authorized users will be allowed to update the system reprogramming and with according to privileges carried by user, system upgrade options will be provided. User privilege and identity will be checked with signature of the message. For managing privacy preservation between owner and other users we will introduce the different session keys for owner and users so that both can have different views of network and can also preserve their privacy from each other.

B. Evaluation Results

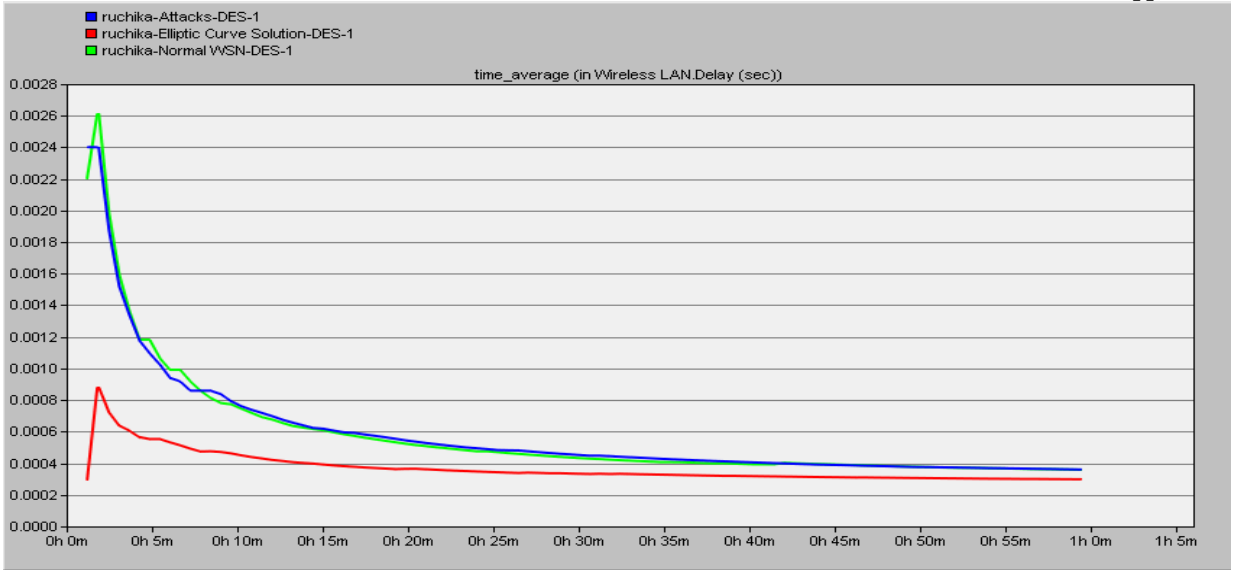
Results obtained for normal performance of wireless sensor network, Performance of wireless sensor network under authentication attack and performance behavior of sensor network with elimination of user authentication attacks with elliptic curve in term of throughput, delay, retransmission attempt, upload response time and download response time is discussed in the following sections.



Performance of sensor network with Throughput of three Scenarios



Performance of sensor network with retransmission attempt of three Scenarios



Performance of sensor network with Delay of three Scenarios

VIII. CONCLUSION & FUTURE SCOPE

In this work, the performance of the wireless sensor network has been summarized. The main focus was to show the performance of sensor network under normal environment, under user authentication attack and performance after elimination of user authentication attack in term of throughput, retransmission attempt, delay, upload response time and download response time. The performance of the network with attack in term of throughput decreases around 51% and with our proposed solution, we have recovered around 49% in throughput. The performance of the network with attack in term of delay decreases around 24% and with our proposed solution, we have recovered around 15% in delay.

It is an important issue for the further study to implement the proposed scheme on the distributed environment of wireless ad-hoc devices. The proposed work focused on the elimination of user authentication attack which based on the concept of single way of authentication attack and have not considered the case of multiple cooperative type of user authentication attack. In future it is very interesting to solve the cooperative user authentication attacks with our proposed scheme. Moreover this research is useful in saving energy but the research is required in case of highly mobile wireless sensor networks such as airborne networks for wireless sensor communication.

REFERENCES

[1] Daojing He, Chun Chen, "SDRP: A Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks", IEEE, Vol.59, No.11, November 2012.

[2] C.Parra and J.Macias,"A protocol for secure and energy-aware reprogramming in WSN",IWCMC,2009,pp.29-297.

[3] Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila,"A Survey of the Elliptic Curve Integrated Encryption Scheme", Journal Computer Science & Engineering, Volume 2, Issue2, August 2010.

[4] E.Thambiraja,Dr. R.Umarani, G.Ramesh,"A Survey on Various Most Common Encryption Techniques",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012.

[5] Cryptographic Message Syntax, Aug. 2002, http://www.ietf.org/rfc/rfc3369.txt IEEE Std 1363-2000, IEEE Standard Specifications for Public-Key Cryptography, IEEE Comp. Soc., Aug. 29, 2000.

[6] Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS),Apr.2002,http://www.ietf.org/rfc/rfc3278

[7] Simar Preet Singh, and Raman Maini, "Comparison of Data Encryption Algorithms" International Journal of Computer Science and Communication Vol. 2, No. 1, pp. 125-127, January-June 2011.

[8] S.Hyun, P.Ning, A. Liu, and W. Du, "Seluge: Secure and dos-resistant code dissemination in wireless sensor networks', in Proc. ACM/IEEEIPSN, 2008, pp. 445-456.

[9] Adam Chlipala, Jonathan Hui, Gilman Tolle"Deluge: Data Dissemination for Network Reprogramming", University of California at Berkeley Computer Science Division Berkeley, CA 94720.

[10] Arikumar, K.S., and Thirumoorthy, K., 2011, "Improved User Authentication in Wireless SensorNetworks" International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT), Tamil Nadu, pp.1011-1015.

[11] Wang, H., Sheng, B., Tan, C., and Li, Q., 2007, "WM-ECC: an Elliptic Curve Cryptography Suite on Sensor Motes" Tech. Rep. WM-CS-2007-11, College of William and Mary, Computer Science, Williamsburg.

[12] Deng, J., Han, R., and Mishra, S., "Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks" The Fifth International Conference on Information Processing in Sensor Networks, Nashville, TN, pp. 292-300.

[13] "An Efficient Protocol for Securing Multiple Patients Privacy in Wireless Body Sensor Network using ECIES" Ramratan Ahirwal Computer Science & Engineering Samrat Ashok Technological Institute Vidisha (M.P.) 464001, India

[14] N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott, andC. Luo.Applicability of identity-based cryptography for disruption tolerant networking. In MobiOpp 2007.

[15] Boneh and M. Franklin M., 2001, "Identity-based encryption from the Weil pairing," Crypto, Proceedings of Crypto 2001 of Lecture Notes in Computer Science ,Vol. 2139, pp. 213–229.

[16] Lanigan, P. E., Gandhi R., and Narasimhan, P., 2006, "Sluice: Secure dissemination of code updates in sensor networks," 26th International Conference on Distributed Computing Systems, pp.53.

[17] S. Capkun, L. Butty´an, and J.-P. ubaux,"Self organized public-key management for mobile ad hoc networks", IEEE TMC 2003.

[18] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE SP 2003.

[19] Hankerson, A. Menezes, and S. Vanstone: Guide to Elliptic Curve Cryptography. Springer

[20] Wikipedia

