International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Bilinear Pairing Based Encryption for Sensor Network

Kelechi Emerole[a]*, Maurice Anyaehie[b], Stanley Nwadike[b]

[a,b]*Department of Electrical and Electronic Engineering, Federal Polytechnic Nekede, Owerri, Nigeria*

[a]*Email: kelechiemerole@gmail.com*

Abstract

In this letter, we review some research efforts in the area of Pairing based encryption for data transmission and storage taking note of the computational overhead and consequently present a simple encryption scheme to buttress our initiative further.

Keywords: network; sensor; cryptography; security; problem; diffie-hellman.

1. Main text

Wireless sensor network is the congregation of small lightweight nodes that communicate through radio links to exchange information about the physical environment they measure. They are made up of a computational device in this case a microcontroller, an n-bit memory and an antenna for transmission of sensory data. Sensors networks are applied in the industry for process monitoring and also in military applications. They are usually deployed in an unsecured manner where they are predisposed to attacks. One of the ways sensors can be attacked is through masquerading where an obnoxious entity pretends to be a legitimate node in a communication network. Such a node can drop data packets instead of forwarding it to the proper destination. Also spoofing attacks are common in sensor networks were confidential data are listened to by an illegitimate node who wants to extract some information from the communication channel. To ensure data integrity and authentication cryptographic primitives are employed. Sensor nodes have limit to their computational abilities because of their energy constrained properties. Cryptographic methods employed should ensure that performance objectives are met in terms of overhead. Cryptography have two broad classes Public Key cryptography and Symmetric Key cryptography employ secret key pairs; public key and secret key. It also employs Public Key infrastructure were a Certificate Authority authenticates the public keys stored in its database.

---

* Corresponding author.

The Certificate Authority signs the public key using digital signature. Public Key cryptography provides the following service authentication and non-repudiation. This is because a separate entity verifies the ownership of the public keys belonging to individual nodes so it is impossible to deny that it is the originator of the data packets or it is the legitimate node on the other end of the communication channel. Also key distribution is enhanced. The key storage with Public key infrastructure pose significant overhead costs and cannot be employed in sensor networks. Also the length of secret keys generated due to large primes can lead to high computational costs. Cryptographic primitive employed in sensor networks should consider the constraints on resources especially eliminating the overhead requirements posed by a public key infrastructure thereby reducing power consumption. Identity-based cryptography meets these requirements. IBC was first proposed by Shamir [1] in his paper in 1984 and stated that secret key pairs can be generated from the identities of the computing entities. The private key generator generates the private key while the public keys are generated from the identities of two communicating nodes. There is no need for a Public Key infrastructure to store the publicly known keys or for distribution.

2. Problem Statement

G_1 and G_2 are prime subgroups of elliptic curve G_m is a subgroup of characteristic 2 or 3 finite field that is F_{2^n} . There are three types of pairing [2] Type 1 pairing; $G_1 = G_2$, Type 2 pairing $G_1 \neq G_2$ and there exists φ a computable homomorphism $\varphi: G_2 \rightarrow G_1$ and Type 3 pairing or asymmetric pairing; $G_1 \neq G_2$ there is no computable homomorphism. Type 1 pairing have been proved to have negligible security [3]. Miller constructed a framework for the efficient calculation of the Weil pairings and Tate pairing on supersingular curve where the embedding degree can either be 1,2,3,4 [4]. Reference [5] followed it up with an algorithm to calculate eta-t(η_T) pairing on supersingular abelian varieties. There have been other efforts to make pairing computation as efficient as possible [6,7]. This efforts are not comparable to the efficient computation of scalar multiplication on elliptic curve which is employed in elliptic curve cryptography. This lays credence to high computation time of the pairing computation which makes pairing cryptography not suitable for wireless sensor network because of its constrained energy requirements. Also pairing require huge memory requirements due to size of the Elliptic curve cryptography library. Efficient software library have been constructed to solve the problem [8]. Also due to resurgence of quantum computers which can solve hard problems in polynomial time there is need to construct public key cryptographic primitives with post quantum cryptographic techniques like Lattices, Multivariate quadratic equations and Quasi-cyclic Low-Density Parity-check codes.

3. Related Works

An identity based encryption scheme was combined with identity based signature scheme with the same public and private key parameters. The signature scheme would be used for verification in the smart collector. The hardness of the Decisional Bilinear Diffie-Hellman problem and the Computational Diffie-Hellman problem was assumed. They also employed the Type-A curves used in PBC. Due to pairing computation they discovered that their computation cost is a little bit larger than standard during the verification process by the collector [9]. The security implications of insider attack, impersonation attack, session key attack and correctness of the analysis using Automated Validation of Internet Security Protocols and Application were analyzed. They

employed bilinear pairing with small parameters for end to end encryption based on the hardness of Decisional Strong Diffie-Hellman assumption and reported that their scheme was secure against Chosen ciphertext and identity attack. They also assumed that the Public Key Generator should be trusted which is not always the case. Hash function computation costs was also assumed to be negligible. From the result of their performance analysis for n number of users , g number of groups and e users in each group the source device computes $(2n + 2g + 2)$ TE exponentiation operations. There was no pairing operation carried out in the encryption phase. For the Decryption phased one modular inversion, one exponential operation, one pairing operation and one hash function [10]. An identity based remote data integrity checking with perfect data privacy preserving for cloud storage with the clause that an external body with the knowledge of cloud user's identity can verify the authenticity of the data was proposed. Zero knowledge method for data confidentiality analysis against the external body was proposed. They employed the notion of asymmetric group key agreement between the third party and the cloud server in their protocol construction. Their security analysis was done using the generic group model. The computation cost of the Key Generating Centre is $2EG_1$ + 1H(two exponential operation in the cyclic group $_1$ and one hash operation). Generating tags for file blocks added to the computational overhead. For n blocks the cost is $(2n + 1)EG_1 + nH$. They also stated that the third party verifier carries out 1 pairing operation and 6 exponentiation in the cyclic group G_1 to challenge queries. This is equivalent to $(c + 1)EG_1 + cP + cH + (c\ 1)E\ G_2$. For the cloud server generating a proof, the computation cost is $2P + (2c–1)MG_1 + EG_2 + MG_2$. They also employed a pseudo random function and a pseudo-random permutation to reduce the communication cost [11]. An identity-based public multi-replica provable data possession scheme was proposed to verify data through a third party without Public key certificate. The soundness and privacy preservation of the security model was analyzed using formal proof. In their analysis, pseudo random functions and arithmetic operation in the finite multiplicative group Z_q^* was not considered. It was reported that the GenProof phase which had a computation cost equivalent to 1Ce+(n+2)$Cexp$+$nCmul$ were n is the challenge block number. The communication cost was reported to be $1G_2 + IG_T + 3log_{2q} + 1Int$ for the challenge phase and IG_2 + 1$Hash$ + 1Sig for the GenProof phase [12]. A revocable identity-based signature scheme with cloud revocation server was proposed and the existentially unforgeability against chosen message and identity attacks security model was analyzed using the random oracle model. They assumed that an untrusted cloud server cannot forge a valid signature even if compromised. They also assumed the hardness of the Computational Diffie-Hellman problem. The order of the groups was set at 512 bits for the cyclic groups while 160 bits for the finite group. They also the computation costs of hash operation to be negligible. The communication costs is equivalent to [G] + [G] + [G] + [q] were [G] is the order size where G is an elliptic curve on finite field F_p [13]. An identity-based signcryption scheme with concealing method for privacy enhancement and data integrity in smart grid communication was proposed. They stated that using minimum spanning trees can lead to efficient communication. The computation costs was equivalent to 4$Tpmul$+1Te for the signcryption phase and 1$Tpmul$ + 4Te in the unsigncryption phase. Their communication cost was equivalent to m + 2[G] [14]. An identity based encryption scheme with equality test in a smart grid environment was proposed. The scheme was proved secured against adaptive chosen ciphertext and identity attack under the random oracle model. They also employed a trapdoor function to carry out equality technique which cannot differentiate the plaintexts if the ciphertexts were given in order to enhance privacy. They assumed the hardness of the Computational Diffie-Hellman problem as their security emphasis. The random prime

number length was set at 512- bit while the order was 160-bit. The computation cost was equivalent to $2Exp + 5M + 2PA + H + h$ for the encryption phase, $2BP + 2M + PA + H + h$ for the decryption phase and $2BP + 2Exp + 2H$ for the Equality Test phase. The communication cost was equivalent to $2[G_1]+2[G_1]+2[Z_q]+[G_1]$[15]. An identity based linearly homomorphic signature scheme employing bilinear groups was proposed. They used the random oracle model to analyse their system against existential forgery on chosen message and identity attack. They assumed the hardness of Computational Diffie-Hellman problem as the basis of the security of their scheme [16].

4. Bilinearity

Assuming G_1 is an additive cyclic group generated by a primitive element g_p and G_2 is an additive cyclic group generated by a primitive element g_q. G_1 and G_2 has a large prime order of p . Let G_m be a multiplicative cyclic order group with a large order prime. A computable bilinear map is defined thus $e\hat{} : G_1 \times G_2 \rightarrow G_m$ with the following properties

- Bilinear: For all random integers a, b $\in_R$ Zp$*$ and $g_p \in G_1$, $g_q \in G_2$ then $e\hat{}(ag_p, bg_q) = e\hat{}(g_p, g_q)^{ab} = e\hat{}(g_p^a, g_q^b)$ holds(symmetric property)
- Non-degenerate: All pairs in the additive cyclic group ($G_1 \times G_2$) are not mapped to the identity element inG_m that is $\hat{e}(g_p, g_q) \neq 1_{G_m}$ for $\hat{e}(g_p, g_q) \in (G_1 \times G_2)$ and 1_{G_m} is an identity element.
- Computability: $\exists$ an algorithm to compute in a probabilistic time $e\hat{}(g_p, g_q)$ for all $g_p, g_q \in G_1, G_2$

Definition 1. *Bilinear group generation probabilistic polynomial time algorithm G on input of a security paramter* 1^{α} *output the* $(G_1, G_2, G_m, \hat{e})$.

5. Security Assumption

Computational Diffie-Hellman Assumption: For some random integers a, b $\in$ Z^*_p and given g_p a primitive element of G_1, given the elements $(g_p, g^a, g^b) \in G_1$ compute g^{ab} in probabilistic polynomial time t is very infeasible. Bilinear Diffie Hellman Assumption: For some random integers a, b, c $\in$ Z^*_p and given g_p a primitiive element of 1, given the elements $(g_p, g_p^a, g_p^b, g_p^c) \in 1$ compute g_p^{abc} in probabilistic polynomial time t is very infeasible

Definition 2 (Negligible function)**.** *A function* $E(\alpha)$ *is called negligible if for every* $v \geq 0$, $\exists$ *a* α_0 such that $E(\alpha) \leq \frac{1}{y}$ *holds for every* $y \geq y_0$.

Definition 3. *A protocol is unforgeable against adaptive chosen plaintext message attack if for any probabilistic polynomial time adversary A the advantage of winning a game corresponding to a set of identities* S^* *is with negligible probability in the security parameter* α

Definition 4. *The protocol is* $(T, E(\alpha), q_s, q_{kg}, q_e, q_d)$ *secure against chosen ciphertext attacks (CCA) if no PPT*

adversary making at most q_s setup queries,q_{kg} key generation queries,q_e encryption queries,q_d decryption queries can win the game with the advantage $Adv^{CCA} = | Pr | d^{'} = d | - \frac{1}{2} | \geq E(\alpha)$

Definition 5. *The protocol is* $(T, E(\alpha), q_s, q_{kg}, q_e, q_d)$ *secure against chosen plaintext attack (CPA) if no PPT adversary making at most q_s setup queries,q_{kg} key generation queries,q_e encryption queries,q_d decryption queries can win the game with the advantage* $Adv^{CP\ A} = | Pr | d^{i} = d | - \frac{1}{2} | \geq E(\alpha)$

6. Security Model

The advantage of the attacker in a sensor network over a legitimate challenger in the sensor network is negligible in the following game. The adversary A chooses a set S^* were $| S^* | \leq N$ and sends S^* to challenger C. The adversary A makes some adaptive queries while the challenger C responds. Setup Query: The challenger C runs the setup and generates (pparams,mpk,msk) were pparams is the system parameters, mpk is the master public key and msk is the master secret key then forwards params and mpk to adversary A while it keeps the confidential the master secret key msk. First Phase Queries: The adversary makes adaptive KeyGen, sign, encrypt, and decrypt queries to challenger in polynomial times as follows KeyGen queries: A queries secret key of Identity ID $\in$ 0, 1^*, the challenger C responds by running the KeyGen algorithm with input ppparams, mpk, msk, ID to output the secret key SK_{ID} and forwards it to the adversary

Hash queries: A queries hash function on message M adaptively in polynomial times and C responds with hashed message to adversary and A stores it in hash list L^{Hi}.

Sign Queries: A makes adaptive queries for a signature on the message M with ID $\in$ 0,1. The challenger C runs the sign algorithm with pparam, M, SK_{ID} and generate signature σ and forwards it to A.

Encrypt queries: C runs the Encrypt algorithm with input pparams, ID, M to generate the ciphertext CT and forwards to A. Decrypt queries: M runs the Decrypt algorithm with pparams, SK_{ID} and CT to generate the message M and forwards to A.

Challenge: A finally outputs ID^*, M_0, M_1,$name^*$to be challenged. Let M_0 and M_1 be two equal length plaintext messages $| M_0 | = | M_1 |$, C responds by choosing a positive integer c *in* 0,1 and running the Encrypt algorithm to generate the challenge ciphertext CT^* on identity ID and message M and forwards to A.

Output: A returns a guess d^i and if d^i = d then wins the game.

7. System Model

The Base Station generates the master public key of the system through the sensor nodes unique identities which is their Medium Access Control addresses and the master secret key. It also uses the master secret key to compute the private secret key. It sends the master public key to all wireless nodes in the network through a secured

channel and keeps the master secret key. The nodes are energy constrained devices that communicate with the Base Station. It receives the secret key from the base station which it employs to encrypt data before sending and decrypt data on receipt.

8. Construction

Setup: The Base station receives an input stimulus in the form of a security parameter α to generate the bilinear public parameters pparams. Let G_1 and G_2 be two cyclic groups and G_m is a cyclic multiplicative group and $\hat{e}: G_1 \times G_1 \rightarrow G_m$ is a bilinear map. G_1 and G_2 have the same order of a large prime p with $p \geq 2^{\frac{\alpha}{2}}$. The Base station chooses a random number $x \in Z_p^*$ and computes g^x as the master secret key and also compute pparam = $\hat{e}(g_p{}^x, g_q{}^x)$. Also let $g_p{}^x$ and $g_q{}^x$ be the primitive element of the two cyclic additive groups respectively. The Base station also chooses cryptographic hash functions; $h_1 : \{0,1\}^* \rightarrow Z_p^*, h_3 : \{0,1\}^n \rightarrow G_m$, $h_4 : G_m \rightarrow \{0,1\}$. The public parameters pparams = (p,g_p, g_q, G_1, G_2,$\hat{e}$, *pparam*, *n*, h_1, h_2, h_3, h_4) is distributed to all the nodes in the network.

KeyGen: The node sends its ID to the Base station which employs the KeyGen algorithm with input identity $ID \in \{0,1\}^n$ for some n, the public parameters pparams and the master secret key g^x then chooses a random integer $r \in Z_p^*$ and computes $SK_{IDi} = (g^x(\mu_o \Pi_i^{\lambda} \mu_i)^r, g^r)$ were $SK_{IDi} = (SK_{IDi,1}, SK_{IDi,2})$.

Encrypt: The node employs the encrypt algorithm with pparams, ID and M as input and chooses a random number $s \in Z_p^*$ to generate ciphertext $CT_{i,1} = M\hat{e}(g^x, h(ID)^s)$, $CT_{i,2} = g^s$ and $CT_{i,3} = (\mu_{oo} \Pi_i^{\lambda} \mu_i)^r g^{h(ID)})$ were $CT = (CT_{i,1}, CT_{i,2}, CT_{i,3})$

Decrypt: The receiving node employs the decrypt algorithm with pparams,, SK_{IDi} and CTas input to generate the plaintext message $M = CTi,1 \quad e\hat{}(SK_{IDi,1}, CT_{i,3} \quad e\hat{}(SK_{IDi,2}, CT_{i,2})$

9. Conclusion

In this letter, we presented a basic encryption scheme with a better computational savings as compared to some reviewed scheme in literature. In the future we will analyze the correctness of our construction

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in Workshop on the theory and application of cryptographic techniques, pp. 47–53, Springer, 1984.

[2] S. D. Galbraith, K. Harrison, and D. Soldera, "Implementing the tate pairing," in International Algorithmic Number Theory Symposium, pp. 324–337, Springer, 2002.

[3] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for cryptogra- phers," Discrete Applied Mathematics, vol. 156, no. 16, pp. 3113–3121, 2008.

[5] P. S. Barreto and M. Naehrig, “Pairing-friendly elliptic curves of prime order,” in International Workshop on Selected Areas in Cryptography, pp. 319–331, Springer, 2005.

[6] E. Lee, H.-S. Lee, and C.-M. Park, “Efficient and generalized pairing computation on abelian varieties,” IEEE Transactions on Information Theory, vol. 55, no. 4, pp. 1793–1803, 2009.

[7] F. Hess, N. P. Smart, and F. Vercauteren, “The eta pairing revisited,” IEEE Transactions on Information Theory, vol. 52, no. 10, pp. 4595– 4602, 2006.

[8] J.-L. Beuchat, J. E. Gonza´lez-D´ıaz, S. Mitsunari, E. Okamoto,

F. Rodr´ıguez-Henr´ıquez, and T. Teruya, “High-speed software imple- mentation of the optimal ate pairing over barreto–naehrig curves,” in International Conference on Pairing-Based Cryptography, pp. 21–39, Springer, 2010.

[9] Z. Wang, “An identity-based data aggregation protocol for the smart grid,” IEEE Transactions on Industrial Informatics, vol. 13, no. 5, pp. 2428–2435, 2017.

[10] D. He, S. Zeadally, B. Xu, and X. Huang, “An efficient identity- based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2681–2691, 2015.

[11] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and

G. Min, “Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 767–778, 2016.

[12] S. Peng, F. Zhou, Q. Wang, Z. Xu, and J. Xu, “Identity-based public multi-replica provable data possession,” IEEE Access, vol. 5, pp. 26990– 27001, 2017.

[13] X. Jia, D. He, S. Zeadally, and L. Li, “Efficient revocable id-based signature with cloud revocation server,” IEEE Access, vol. 5, pp. 2945– 2954, 2017.

[14] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, “Cyber security and privacy issues in smart grids,” IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 981–997, 2012.

[15] L. Wu, Y. Zhang, K.-K. R. Choo, and D. He, “Efficient identity-based encryption scheme with equality test in smart city,” IEEE Transactions on Sustainable Computing, vol. 3, no. 1, pp. 44–55, 2017.

[16] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, “An id- based linearly homomorphic signature scheme and its application in blockchain,” IEEE Access, vol. 6, pp. 20632–20640, 2018.