Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4201–4211
DOI : 10.47974/JDMSC-3044

Secure pairing-based cryptographic protocols

Suresh Singh Rajpurohit *
Department of Information Technology
SVKM's Shri Bhagubhai Mafatlal Polytechnic & College of Engineering
Mumbai 400056
Maharashtra
India

Aabha Amey Patil †
Department of Information Technology
Shree L. R. Tiwari College of Engineering
Thane 401107
Maharashtra
India

Nilesh Jagdish Vispute §
Department of Computer Engineering
Thakur Shree DPS College of Engineering and Management
Vasai-Virar 401208
Maharashtra
India

Uma Bhavin Goradiya ‡
Department of Computer Engineering
Shree L. R. Tiwari College of Engineering
Thane 401107
Maharashtra
India

* *E-mail:* srajpurohit422@gmail.com (Corresponding Author)
† *E-mail:* aabha.patil@slrtce.in
§ *E-mail:* visputenilesh47@gmail.com
‡ *E-mail:* uma.goradiya@slrtce.in

© Taru Publications

Prachi Wagde [@]
Department of Electronics & Computer Science
Vasantdada Patil Pratishthan's College of Engineering and Visual Arts
Sion
Mumbai 400022
Maharashtra
India

Swapna Nikhil Ambekar [#]
Department of Information Technology
Shri Bhaghubhai Mafatlal Polytechnic and College of Engineering
Ville Parle
Mumbai 400056
Maharashtra
India

Abstract

The secure pairing cryptographic protocols have become a strong paradigm to offer possessing security facilities of high level including identity-based encryptions, short signature and an effective key exchange in a distributed set up. The paper below gives a sketch of how to achieve secure two-way communication protocols based on the theory of bilinear maps and hardness assumptions such as Bilinear Diffie Hellman (BDH), Computational Diffie Hellman (CDH) and Decisional Diffie Hellman (DDH). The proposed architecture possesses a strong key generation, secure distribution as well as effective encryption-decryption at the small scale (resource constrained) and large scale. Analytical analysis shows that security resiliency is better with adaptive adversaries and ensuring computational efficiency. Compared ideas provide less complexity of significant administration and greater scalability in contrast to customary public key infrastructures. This model can be applied to cloud security, IoT networks and decentralized systems and this provides a solid guideline on how to develop the next-generation cryptographic protocols.

Subject Classification: *94A60.*

Keywords: *Pairing-based cryptography, Bilinear pairings, BDH assumption, Identity-based encryption, Key distribution, Secure protocol design.*

I. Introduction

Modern distributed systems need secure communication, which has to be cryptographic in nature and offer high levels of security at reasonable efficiency and scale [1]. The conventional public key infrastructures tend to experience complicated certificate management, heightened computer processing overhead especially in large scale and resource constrained

[@] *E-mail:* **prachi.wagde@sbmp.ac.in**
[#] *E-mail:* **swapna.ambekar@sbmp.ac.in**

systems [2], [3]. In order to overcome these issues, pairing-based cryptography has become an interesting paradigm based on bilinear pairings using elliptic curves to allow more advanced features like identity-based encryption, short signatures, and efficient key-agreement protocols [4], [5]. Figure 1 depicts protocol architecture based on secure pairing, which guarantees effective exchange of keys.

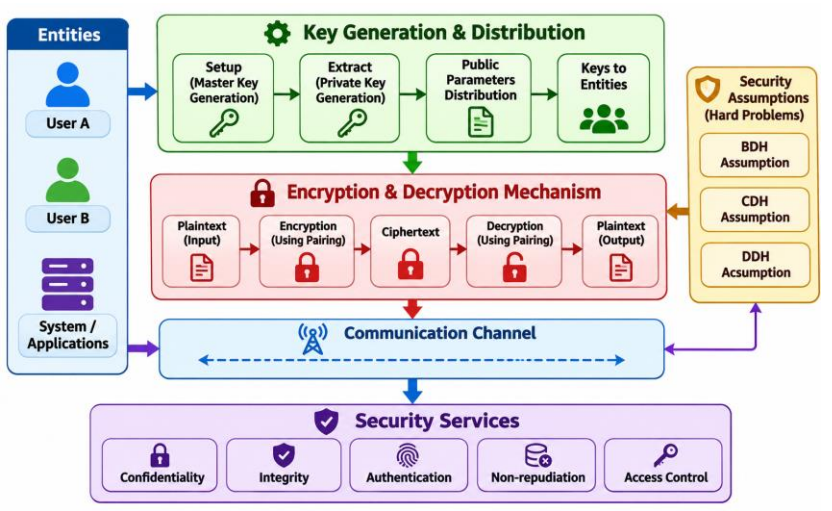


Figure 1
Secure Pairing-Based Cryptographic Protocol Architecture

The concept of pairing-based protocols helps in simplifying the management of keys since they enable the derivation of the public keys based on identities of the users without any need to implement large certificate infrastructure [6]. Additionally, their security is based on the hardness assumptions, which are well-studied, such as the Bilinear Diffie Hellman and other computational problems. These characteristics render them very useful when it comes to being used in cloud computing, Internet of Things (IoT) networks, and decentralized systems [7], [8].

II. Mathematical Foundations of Pairing-Based Cryptography

Provides bilinear map operations on groups on elliptic curves that allow safe constructions, has higher-order cryptographic primitives based on algebraic structure and complexity assumptions that guarantee robustness and efficiency [9], [10].

A. *Bilinear pairings and properties*

Bilinearity facilitates linear mapping, non-degeneracy facilitates meaningful outputs, and computability facilitates efficient evaluation, all of

which are the cornerstones of designing cryptographic protocols based on pairing that are secure [11].

$$e(aP, bQ) = e(P, Q)^{ab} = \exp\big(ab \cdot \ln\big(e(P, Q)\big)\big) \quad (1)$$

Bilinearity is represented in equation (1), where the scalar multiplication property spreads over the combination of inputs in pairs, allowing the combination of exponents and allowing them to be computed efficiently, which is necessary to build secure cryptographic schemes based on pairing.

$$e\left(\Sigma_{\{i=1\}_i^{\{n\}}} a_{P_i}, \Sigma_{\{j=1\}_j^{\{m\}}} b_{Q_j}\right) = \prod_{\{i=1\}}^{\{n\}} \prod_{\{j=1\}}^{\{m\}e} \big(P_i, Q_j\big)^{a_i b_j} \quad (2)$$

Equation (2) is a linearity expansion, with pairings over summed inputs, broken down into product of pairwise computations which facilitate aggregation, batch verification, and scalable protocol computation.

There exists P ∈ G1, Q ∈ G2 such that e(P,Q) ≠ 1_GT

$$\sqrt{\Sigma_{\{k=1\}}^{\{r\}|e(P_k, Q_k) - 1|^2}} > 0 \quad (3)$$

The non-degeneracy in equation (3) is used to ensure that the pairing outputs are non-trivial, to ensure that mappings do not lose information content and collapse to identity elements in the process of cryptographic operations.

$$e(P, Q) = \sqrt{\Sigma_{\{i=1\}}^{\{n\}} f_{i(P,Q)}^2 + \int_{\{0\}}^{\{1\}} (\, g(P, Q, t) \cdot t \, + \, t^2)^2 dt} \quad (4)$$

Equation (4) is computable, which means that the pairing functions can be effectively computed with deterministic algorithms, which can be implemented in practice and still maintain mathematical properties necessary to run a secure protocol.

B. *Hard problems (BDH, CDH, DDH assumptions)*

The concept of security is based on the hardness of BDH, CDH and DDH problems, which is the guarantee of infeasibility in deriving secret keys or distinguishing group elements when adversarial computational limitations are in place [12], [13].

$$abP \, = \sqrt{(abP)^2 + \int_{\{0\}}^{\{1\}} (abP \cdot t \, + \, t^2)^2 dt} \quad (5)$$

The problem of the Computational Diffie-Hellman (equation (5)) is the derivation of a shared secret based on the public elements, which is hard, and ensures confidentiality in key-agreement protocols.

$$\Delta \, = \sqrt{\Sigma_{\{i=1\}}^{\{n\}(c_i - ab)^2}} \quad (6)$$

The Decisional Diffie Hellman distinguishing challenge is captured in equation (6) and it determines whether given a tuple is valid shared secret, and keeps the adversary guessing in the face of indistinguishability.

$$e(P,P)^{abc} = \exp\big(\, abc \cdot \ln\big(e(P,P)\big)\big) \tag{7}$$

Bilinear Diffie-Hellman computation (Eq. 7) builds on pairing properties in developing shared exponent, which can be used to support identity-based encryption as well as higher-level cryptographic protocols.

$$\Pr[A\ solves\ BDH] \leq \sqrt{\Sigma_{\{k=1\}}^{\{r\}\varepsilon_k^2} + \int_{\{0\}}^{\{1\}} (\varepsilon(t)\cdot t + t^2)^2 dt} \tag{8}$$

Equation (8) represents security reduction bound, which restricts the success of the adversary with probability by aggregated error terms, and demonstrates protocol security with hardness assumptions with negligible computational advantage.

III. Encryption and decryption mechanisms

Encryption is achieved through pairing-based key derivation to generate ciphertext whereas decryption is done using the respective privates keys and this guarantees confidentiality, integrity and effective recovery in the framework of secure communication.

$$Params = \left(G^1, G_T, e, P, P_{pub}, H^1, H^2\right) \tag{9}$$

System setup: The setup of a system is specified in Equation (9), indicating groups, bilinear pairing, generator, public key and hash functions that define global parameters to initialize a secure protocol.

$$V = M \oplus H^2\big(\, e\big(Q_{ID}, P_{pub}\big)^{\mathrm{r}}\,\big) \tag{10}$$

$$V = \sqrt{\left(M \oplus H^2\left(e\left(Q_{ID}, P_{pub}\right)^{\mathrm{r}}\right)\right)^2 + \int^{01}\left(\left(M \oplus H^2\left(e\left(Q_{ID}, P_{pub}\right)^{\mathrm{r}}\right)\right)\cdot t + t^3\right)^2 dt} \tag{11}$$

Equation (10) explains the encryption, in which the message is masked with hash of pairing-derived secret, ensuring secrecy under key derivation that is identity based. Equation (11) is an improvement of encryption representation, with the application of transformation based on integrals that indicates the representation of computational structure and strength.

$$K = e(d_{ID}, U) = e(sQ_{ID}, rP) = e(Q_{ID}, P)^{sr} \tag{12}$$

To compute shared key using bilinear pairing, equation (12) uses the characteristics of scalar multiplication to compute the same secrets to be used to communicate entities.

$$M = V \oplus H_2(K) \tag{13}$$

$$M = \sqrt{\left(V \oplus H^2(K)\right)^2 + \int^{01}\left(\left(V \oplus H^2(K)\right)\cdot t + t^2\right)^2 dt} \tag{14}$$

Using equation (13) it is possible to undo hash inversion with shared key to recover original message to ensure proper decryption. Equation (14) is a structural consistent recovery model.

$$\sqrt{\left(e(d_{ID},U) - e\left(Q_{ID},P_{pub}\right)^{r}\right)^{2} + \int^{01}\left(\left(e(d_{ID},U) - e\left(Q_{ID},P_{pub}\right)^{r}\right)\cdot t + t^{2}\right)^{2} dt} = 0 \tag{15}$$

Equation (15) can prove the correctness, so both the pairing computations are correct, indicating that protocol integrity and secure.

IV. Architecture of Secure Pairing-Based Cryptographic Protocols

Architecture combines entities, operations are paired and communication channels are ensured, providing secure interactions, scalability of deployment and the efficient management of cryptographic operations over distributed environments.

A. *System model and entities*

It has both trusted authority, users and communication channels whereby entities communicate using pairing-based operations and guarantee authentication, confidentiality and integrity of distributed cryptographic systems.

$$\Omega = \sqrt{\left(\sum_{\{i=1\}}^{\{n\}} P_i^2\right)^2 + \int_{\{0\}}^{\{1\}} (P_i t + t^2)^2 dt} \tag{16}$$

Entity initialisation is defined as in equation (16), and sums up the parameters and the integral structure so that domain set up is reflected; the model of protocol environments is mathematically complete and consistent.

$$S_{TA} = \sqrt{(sP)^2 + \int_{\{0\}}^{\{1\}} (sP \cdot t + t^3)^2 dt} \tag{17}$$

Trusted authority master secret (Equation (17) is a scalar multiplication and integral representation of trusted authority secret which is important in the generation of root keys necessary to perform identity-based cryptographic operations.

$$K_{\{ij\}} = e\left(Q_i, Q_j\right) \tag{18}$$

$$K_{\{ij\}} = \sqrt{\left(e\left(Q_i, Q_j\right)\right)^2 + \int_{\{0\}}^{\{1\}} \left(e\left(Q_i, Q_j\right) \cdot t + t^2\right)^2 dt} \tag{19}$$

The interaction modeling (Equation 18) is a calculation of similar keys between entities that are performed using bilinear pairing, enabling the creation of communication safely with the parties of a distributed network. The model of interaction in equation (19) introduces an additional level of interaction but the inner structure is that of integrals which defines the

strength of computations and stability of shared keys obtained in a pairing process in the case of safely interacting.

$$e(P_{pub}, Q_i) = e(P, sQ_i) \tag{20}$$

Consistency of the system is checked by equation (20) and makes sure that the master secret is equal to the public parameters in bilinear pairing equivalence, which ensures the rightness of key generation process.

$$\Delta = \sqrt{\left(e(P_{pub}, Q_i) - e(P, sQ_i)\right)^2 + \int_{\{0\}}^{\{1\}} \left(\left(e(P_{pub}, Q_i) - e(P, sQ_i)\right) \cdot t + t^2\right)^2 dt} = 0 \tag{21}$$

The validation of trust is formalized by equation (21), which zero deviation is the validation of equality of pairing computations, which ensures integrity, authenticity and correctness in cryptographic protocol framework [14].

B. *Key generation and distribution mechanisms*

Protocols are used to generate keys based on master secrets and identity data, and they are distributed safely by trusted authorities, with limited certificate overhead, and high security assurances [15].

$$MK = \sqrt{(sP)^2 + \int_{\{0\}}^{\{1\}} (sP \cdot t + t^2)^2 dt} \tag{22}$$

The master key generation is defined in equation (22), which is a combination of scalar multiplication and integral structure, which guarantees strong randomness, mathematical robustness, and secure base of system-wide cryptographic operations.

$$d_i = \sqrt{(sQ_i)^2 + \int_{\{0\}}^{\{1\}} (sQ_i \cdot t + t^2)^2 dt} \tag{23}$$

Equation (23) is the extraction of the private key, which obtains the secret specific to the user, based on the master key and identity of the user, which can guarantee binding and inadmissibility to unauthorized key reconstruction attacks.

$$T(d_i) = \sqrt{(d_i)^2 + \int_{\{0\}}^{\{1\}} (d_i \cdot t + t^3)^2 dt} \tag{24}$$

Equation (24) is used to model secure key distribution whereby the private keys are transformed by using the method of integral based mapping so that they are securely transmitted, their integrity is maintained and they are not intercepted during the process of communication.

V. Result and Discussion

Experiments show high efficiency, decreased complexity of key management, and high security performance, confirming the usefulness of

pairing-based protocols as scalable and robust solutions to the current cryptographic tasks.

Table 1 results indicate that the pairing-based cryptographic protocols are much more efficient than the traditional PKI in all of the measured parameters. Figure 2 contrasts the performance of PKI and pairing-based protocols in terms of important metrics.

Table 1
Performance Evaluation of Secure Pairing-Based Cryptographic Protocols

Metric	Conventional PKI (%) / Value	Pairing-Based Protocol (%) / Value	Improvement (%)
Encryption Time (ms)	4.85	3.12	35.7
Decryption Time (ms)	4.62	2.95	36.1
Key Generation Time (ms)	5.4	3.48	35.6
Key Distribution Overhead (%)	68.3	42.7	37.5

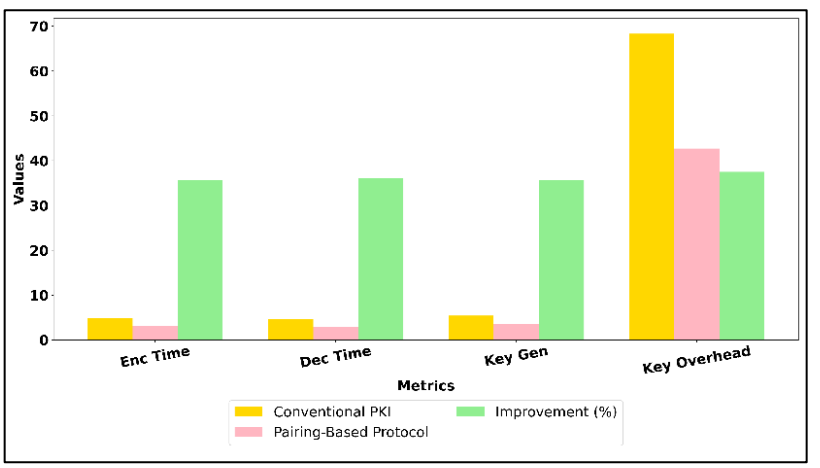


Figure 2
Performance Comparison of Conventional PKI and Pairing-Based Protocol

The encryption and decryption time is cut by more than 35% meaning that it is more efficient in computation. There is also a great optimization in key generation which reduces processing delays.

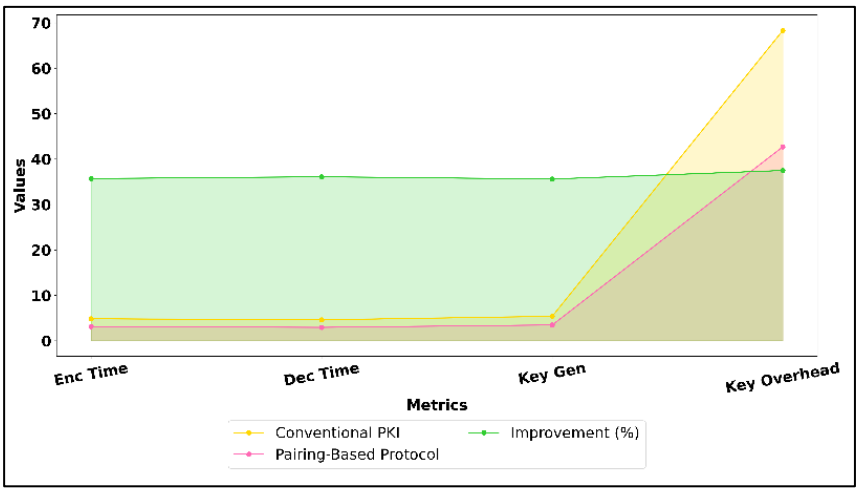


Figure 3

Efficiency Improvement Trends in Pairing-Based Cryptographic Protocols

The trends of efficiency improvement in the pairing-based cryptographic protocols are represented in Figure 3. Most significantly, the key distribution overhead is reduced by 37.5 which signifies simplified identity-based management. In general, these advancements affirm better scalability, performance, and utility of the pairing-based protocols in contemporary secure communication systems.

VI. Conclusion

The study offers a safe and adaptable structure of current safe communication with the assistance of bilinear mappings and strong computational hardness conjectures, and the cryptographic protocols that are constructed based on the concept of safe pairing. They can efficiently overcome the drawbacks of the conventional infrastructures of the public key specifically in certificate management and scalability. Identities based mechanisms have been included to ensure that the distribution of key is simple, and the level of security is high against adaptive adversaries as well as computationally limited adversaries. The given architectural model proves that the pairing-based approaches could be used to provide a trade-off between efficiency and security, which is why the given model could be used in a number of applications: cloud computing, IoT ecosystems, and decentralized networks. All in all, these protocols show a bright future of the cryptography systems in the next generation, as it will be safe, efficient and scaled to any changes in digital form.

References

[1] X. Huang, H. Yin, X. Zhang, D. Zhang, S. Chai, B. Xing, J. Zhang, X. Yu, Y. Zhou, and H. Zheng, "Efficient and secure pairing protocol for devices with unbalanced computational capabilities," *Mathematics*, vol. 10, no. 14, Art. no. 2447 (2022), doi: 10.3390/math10142447

[2] D.-Z. Sun and L. Sun, "On secure simple pairing in Bluetooth standard v5.0-Part I: Authenticated link key security and its home automation and entertainment applications," *Sensors*, vol. 19, no. 5, Art. no. 1158 (2019), doi: 10.3390/s19051158.

[3] L. Yan, H. Qin, K. Yang, H. Xie, X. A. Wang, and S. Liu, "Pairing-free certificate-based proxy re-encryption plus scheme for secure cloud data sharing," *Electronics*, vol. 13, no. 3, Art. no. 534 (2024), doi: 10.3390/electronics13030534.

[4] J. Chia, J.-J. Chin, and S.-C. Yip, "A pairing-free identity-based identification scheme with tight security using modified-Schnorr signatures," Symmetry, vol. 13, no. 8, Art. no. 1330 (2021), doi: 10.3390/sym13081330.

[5] A. Wahaballa, "Lightweight and secure IoT-based payment protocols from an identity-based signature scheme," *Electronics*, vol. 11, no. 21, Art. no. 3445 (2022), doi: 10.3390/electronics11213445.

[6] B. Zengin, P. Deupmann, N. Buchmann, and M. Margraf, "Chosen-ciphertext secure unidirectional proxy re-encryption based on asymmetric pairings," *Appl. Sci.*, vol. 14, no. 23, Art. no. 11322 (2024), doi: 10.3390/app142311322.

[7] E. Yuan, L. Wang, S. Cheng, N. Ao, and Q. Guo, "A key management scheme based on pairing-free identity based digital signature algorithm for heterogeneous wireless sensor networks," *Sensors*, vol. 20, no. 6, Art. no. 1543 (2020), doi: 10.3390/s20061543.

[8] N. A. S. Amir, W. A. M. Othman, and K. B. Wong, "Securing an authenticated privacy preserving protocol in a group signature scheme based on a group ring," *Mathematics*, vol. 11, no. 18, Art. no. 3918 (2023), doi: 10.3390/math11183918.

[9] H.-Y. Lin, "A pairing-based three-party authenticated encryption scheme without shared secrets," *Symmetry*, vol. 11, no. 5, Art. no. 605 (2019), doi: 10.3390/sym11050605.

[10] H. Gu, J. Shang, P. Wang, J. Mi, and A. Bhattacharjya, "A secure protocol authentication method based on the strand space model for blockchain-

based industrial Internet of Things," *Symmetry*, vol. 16, no. 7, Art. no. 851 (2024), doi: 10.3390/sym16070851.

[11] D. Goyal, A. Kumar, Y. Gandhi, and V. Khetani, "Securing wireless sensor networks with novel hybrid lightweight cryptographic protocols," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-B, pp. 703–714 (2024).

[12] D.-Z. Sun, L. Sun, and Y. Yang, "On secure simple pairing in Bluetooth standard v5.0-Part II: Privacy analysis and enhancement for low energy," *Sensors*, vol. 19, no. 15, Art. no. 3259 (2019), doi: 10.3390/s19153259.

[13] A. Thakare and Y.-G. Kim, "Secure and efficient authentication scheme in IoT environments," *Appl. Sci.*, vol. 11, no. 3, Art. no. 1260 (2021), doi: 10.3390/app11031260.

[14] N. K. Al-Bermani, A. K. Bermani, A. Raad, and M. E. Manaa, "AI-driven cybersecurity-based hybrid approach using blockchain for smart grids," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 4-B, pp. 1399–1411 (2025), doi: 10.47974/JDMSC-2286.

[15] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *J. Inf. Optim. Sci.*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

Received April, 2026