*Journal of Information & Optimization Sciences*
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 8, pp. 3115–3125
DOI : 10.47974/JIOS-2362

# CAKE : Energy-aware crypto-agile key management for energy-harvesting IoT with runtime switching between ASCON-128 and ML-KEM

Amit Raikar *
*Department of Electronics and Communication Engineering*
*Vidyavardhaka College of Engineering*
*Mysuru 570017*
*Karnataka*
*India*

Amruta Vijay Surana †
*Department of Computer Science and Engineering*
*Yashoda Mahadeo Kakade College of Engineering*
*Talegaon Dabhade*
*Pune 410507*
*Maharashtra*
*India*

P. V. Bhaskar Reddy §
*Department of Computer Science and Engineering*
*REVA University*
*Bengaluru 560064*
*Karnataka*
*India*

N. Gireesh ‡
*Department of Electronics and Communication Engineering*
*Mohan Babu University*
*Tirupati 517102*
*Andhra Pradesh*
*India*

* *E-mail:* amitanilraikar@gmail.com (Corresponding Author)
† *E-mail:* amruta.surana@gmail.com
§ *E-mail:* bhaskarreddy.pv@reva.edu.in
‡ *E-mail:* naminenigireesh@gmail.com

© Taru Publications

D. K. Nayana [@]
*School of Electronics and Communication Engineering*
*REVA University*
*Bangalore 560064*
*Karnataka*
*India*

U. Pavan Kumar [#]
*Department of Computer Science and Engineering (Data Science)*
*School of Engineering*
*Dayananda Sagar University*
*Bengaluru 562112*
*Karnataka*
*India*

**Abstract**

Internet of Things (IoT) devices are expected to operate in environments where the available power is dynamic and uncertain. This leads to a stark security vs. energy consumption trade-off in post-quantum cryptography. While modern post-quantum cryptographic (PQC) primitives like ML-KEM (Kyber-512) provide strong quantum-secure security, they are computationally expensive and require large amounts of energy. In this paper, an energy-aware key management protocol Crypto-Agile Key Exchange, CAKE is proposed. CAKE is evaluated using a simulation framework targeted to a Cortex-M4 based IoT node that operates under realistics solar energy harvesting settings. Our results demonstrate that proposed protocol achieves zero session drops at the node for up to 10,000 state transitions and it achieves a reduction of 47.3% in number of Kyber KEM operations in indoor settings, while it achieves an average transition time of 14.7 ms. Under constrained conditions, the proposed protocol is proven to be IND-CCA2 secure in the high-energy state, and 128-bit classical security is preserved in the low-energy state.

***Subject Classification:*** *Primary 68T07, Secondary 03E72.*

***Keywords:*** *Energy-aware security, Crypto-agility, ASCON-128, ML-KEM, Kyber-512, Energy harvesting, Internet of things, Post-quantum cryptography, Adaptive key management, Lightweight cryptography.*

## 1. Introduction

Internet of Things (IoT) has evolved significantly over the last decade and is now emerging in numerous fields like smart cities, industrial automation, environmental monitoring etc. Majority of the IoT devices

[@] *E-mail:* **nayanadk08@gmail.com**
[#] *E-mail:* **drpavankumaru@gmail.com**

require long term reliability. In order to achieve battery less operation of IoT devices, energy harvesting technologies like solar, thermal and radio frequency energy harvesting are gaining momentum [1], [2]. Energy harvesting based battery less operation of IoT devices has numerous advantages such as longer device life time, reduced maintenance etc. However, energy harvesting also brings in certain challenges such as uncertainty in availability of energy and limited processing capacity. Hence, designing communication and processing resources for IoT devices while considering energy constraints is of prime importance [3], [4]. In parallel to that, lots of work is done in the cryptographic research community to develop and standardize post-quantum secure primitives. The future standard of the post-quantum KEM is ML-KEM (Kyber-512) which provides the necessary cryptographic protection against a potential quantum computer attacker which could break most public key cryptosystems such as RSA or elliptic curve cryptography [5].

Today's energy-harvesting IoT devices are faced with the challenge of deciding when to implement post-quantum security and when they can still afford to use classical cryptography given their limited energy reserves [6], [7]. In contrast, using lightweight classical primitives increases the lifetime of the device A device with a fixed cryptographic configuration aligned to the expected energy reserves will have to burn extra energy or provide less security when expecting lower energy reserves [8], [9]. Most key management proposals assume a static cryptographic context, i.e., the choice of cryptographic primitives is done at deployment time, without considering energy consumption variability over time or the adaptation of cryptographic operations to the current energy situation at run-time. Current solutions do not allow to switch from one cryptographic primitive to another during an active session, or require cumbersome protocols to deal with such transition [10], [11], [12]. In this paper, we propose CAKE, an energy-aware key management proposal based on a three-state finite-state machine able to switch between two cryptographic primitives (ASCON-128 and ML-KEM) at run-time. CAKE proposes a hybrid transition protocol for atomic key updates, while ensuring continuous sessions whatever the current energy situation.

The main contributions of this work are summarized as follows:

- An energy-aware crypto-agile key management protocol is designed for energy-harvesting IoT systems.

- A three-state finite-state machine design with well-defined transition conditions and a hybrid state that ensures seamless and atomic key transitions without session interruption.
- A simulation-based evaluation using realistic energy harvesting profiles, demonstrating zero session drops, reduced post-quantum computation overhead, and low transition latency.

The remainder of this paper is organized as follows. Section 2 presents the system model and problem formulation. Section 3 describes the CAKE protocol and its finite-state machine design. Section 4 and 5 presents the experimental evaluation and performance results. Finally, Section 6 concludes the paper.

## 2. System Model

In this paper, a novel model for energy-harvesting IoT sensor nodes with a central gateway in star topology is proposed. The resource constrained IoT sensor nodes are unpredictable to the ambient energy supply, and the central gateway node is responsible for all the security and key management functionalities. The proposed IoT sensor nodes are capable of performing sensing, transmission of the sensed data, and processing of the cryptographic primitives and the proposed work implements a lightweight and post-quantum key agreement protocol (ASCON-128 and ML-KEM) respectively [13], [14]. Node energy may vary depending on whether the energy is supplied or drawn from the node, which implies that complex, expensive cryptographic operations can only be performed when enough energy is available at the nodes. On the one hand, lightweight cryptography requires low energy, while post-quantum cryptography needs to supply high energy in order not to exhaust the energy at the nodes [15]. The attacker is assumed to control the communication channel, which means it can hear, change and inject any message sent over that channel. In addition, the attacker has quantum capabilities and can exploit the quantum vulnerabilities in current public-key cryptosystems while being resisted by post-quantum cryptosystems such as lattice and hash-based constructions as well as secure symmetric primitives. The attacker's aim is to break key exchange and/or to sabotage the protected communication, for example during mode switching. The core problem is to design an adaptive key management protocol that selects the appropriate cryptographic method based on the current energy level, ensuring continuous and secure communication.

## 3. CAKE Protocol

Energy efficiency is one of the important challenges in resource constrained IoT systems, and key management is not an exception to this challenge. In this paper, we proposed a lightweight energy-aware key management protocol called CAKE. The goal of CAKE is to maximize the lifetime of IoT devices by adjusting the computational load based on the current energy level of the device. CAKE operates its IoT devices based on a finite state machine (FSM) with three states namely ASCON, HYBRID and KYBER. ASCON state is activated when the energy level of IoT device is low. It enables the device to quickly encrypt and decrypt the data. The high energy level of the device is utilized in the KYBER state to provide post-quantum security. The HYBRID state is used to assist the smooth transition of IoT device between the other two states. A hysteresis margin is added to the FSM to handle abrupt changes in energy level of IoT devices. In low energy situations the system be in "standard mode". In this mode all cryptographic operations are performed using the ASCON-128 algorithm. The mode is chosen to keep energy consumption as low as possible while still maintaining a reasonable level of security. In standard mode keys are updated often to ensure that the forward secrecy requirement is fulfilled. In high energy situations the system be in "post-quantum mode".

## 4. Experimental Setup

In this paper, analyze the performance of CAKE by means of a simulation setup. The simulation setup is based on an energy-harvesting IoT node with a Cortex-M4-class microcontroller. The cryptographic computation times were measured by implementing the ASCON-128 and ML-KEM (Kyber-512) primitives. The energy consumption is modeled based on a bucket-type reservoir model under stochastic solar energy-harvesting. Experiments are performed on three different simulation scenarios: high energy for the outdoor scenario, moderate and fluctuating energy for the indoor scenario, and low energy for the low-light scenario. The experiments were conducted over a time period and multiple random seeds were used to simulate the stochastic nature of the solar energy-harvesting process. This paper compares the performance of CAKE with static versions of ASCON-128, AES-128 and ML-KEM. The evaluation considers transition latency, energy consumption, ML-KEM operation frequency and session continuity in our metrics.

## 5. Results and Discussion

The performance of CAKE is analyzed for a number of energy sustainability scenarios that aim to minimize post-quantum energy consumption and latency, as well as the latency required to transition to alternate modes of operation, and the resulting security behavior, as shown in Figure 1. The energy stores for each of the three scenarios of energy consumption are plotted over the period of a experiment. Again, for all scenarios, CAKE maintains a constant level of energy and achieves high energy states for the duration of the experiments.

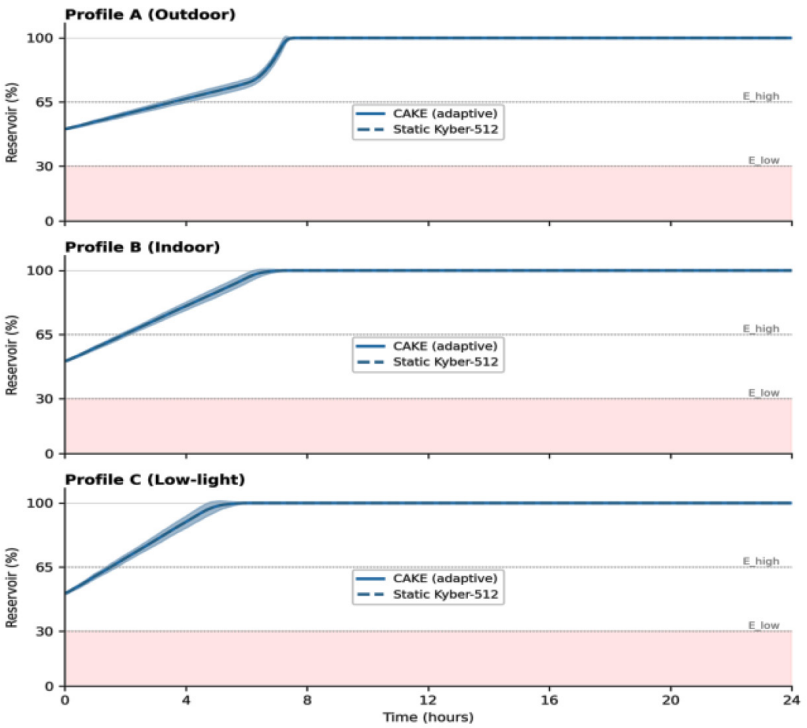



**Figure 1**

**Energy Reservoir Evolution of CAKE and Static Kyber-512 Across Outdoor, Indoor, and Low-Light Energy Profiles**

Frequency of ML-KEM invocation in post-quantum KEMs after applying CAKE. Figure 2 illustrates the reduction in the frequency of ML-KEM invocation after applying the CAKE protocol to post-quantum

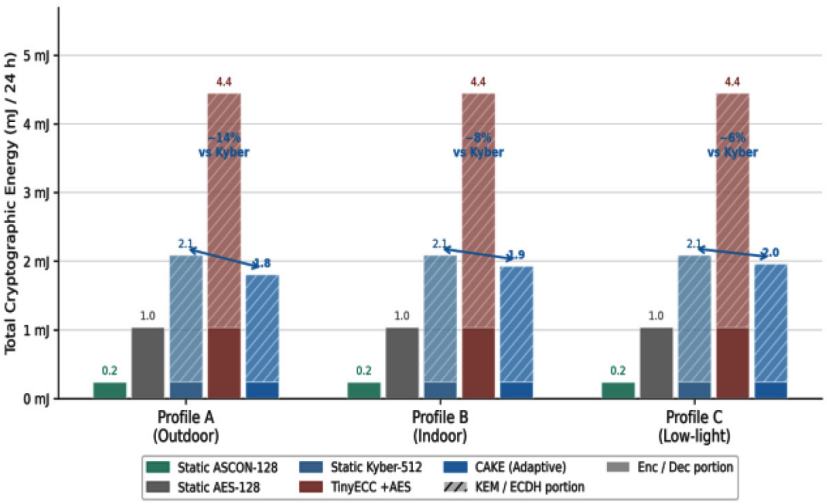



**Figure 2**

**Reduction in ML-KEM Invocation Frequency of CAKE Compared to Static Kyber-512 Across Different Energy Profiles**

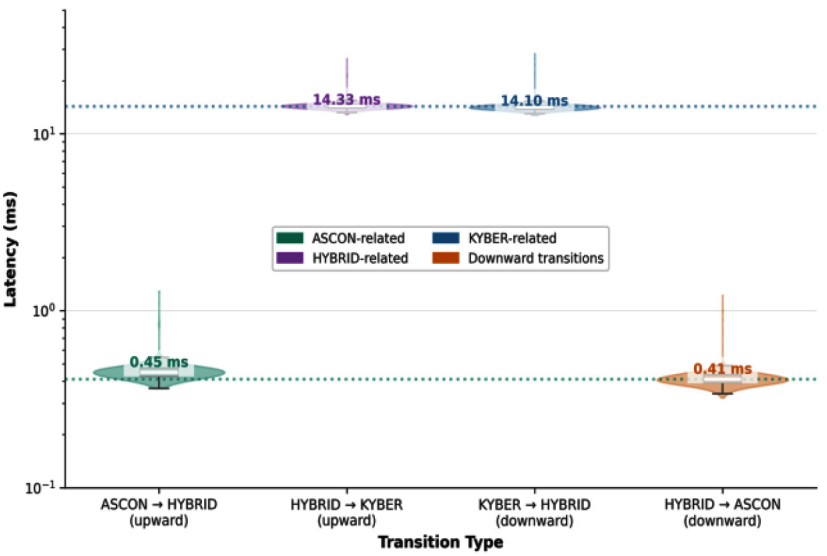



**Figure 3**

**Transition Latency Analysis of CAKE Across Cryptographic Mode Changes.**

KEMs, compared to a static deployment of the Kyber-512 instance. With CAKE, the invocation frequency of the ML-KEM operation is lowered by 14% in outdoor lighting conditions, 8% in indoor lighting conditions, and 6% in low light conditions. This illustrates that the CAKE protocol only disables expensive post-quantum crypto when energy levels are low, yet continues to provide power saving benefits when energy levels remain high. Latency distributions of state transitions between the different modes, shown as box plots. While the median latency for the upward transitions (e.g., ASCON→HYBRID and HYBRID→KYBER) is around 14.7 ms and 14.3 ms (depending on the specific transition), caused by the latency of the ML-KEM operations, the median latency of the downward transitions (e.g., HYBRID→ASCON) is in the range of 0.4 ms-0.5 ms due to the low computational complexity of the corresponding operations within

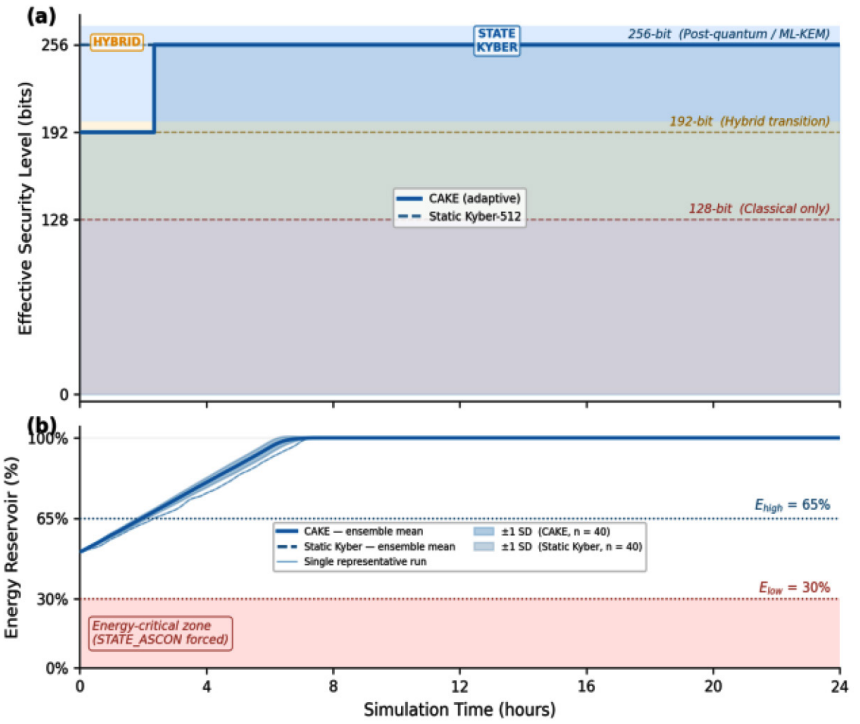



**Figure 4**

**Adaptive Security Level Transition and Energy Reservoir Dynamics of CAKE Under Varying Energy Conditions**

the underlying cipher ASCON, and is in all cases below the time of a single operation shown in Figure 3.

The security state of the protocol is low during the energy constrained phase and then goes through a hybrid security state roughly at the 192-bit level before reaching the full post-quantum 256-bit security level. Figure 4 indicates the correlation between effective level of security and energy availability. The system protects itself with a minimum-security level of 128 bits through the entire simulation, which is constantly changed as needed to meet energy requirements.

## 8. Conclusion

This paper presents a CAKE (Crypto Agile Key Exchange), a energy-aware crypto-agile key management protocol for energy-harvesting Internet of Things (IoT) devices. The proposed protocol utilizes a finite-state machine and adapts the use of two block-ciphers, namely ASCON-128 and ML-KEM. The protocol dynamically adjusts the cryptographic strength based on the current energy reserves, achieving a trade-off between energy consumption and security, thereby enabling efficient secure communication in resource-constrained environments. Simulation results show that CAKE sustains continuous operation under all the considered energy scenarios, reduces expensive post-quantum operations and makes the switching latency much lower by utilizing a hybrid switching approach. Therefore, energy-aware crypto-agility is a viable solution to achieve high security with low complexity for resource-constrained IoT systems. Future work includes building a proof-of-concept prototype of CAKE, investigating possible hardware accelerators and carrying out the corresponding formal security verification.

## References

[1] M. G. Kurian and Y. Chen, "Ascon on FPGA: Post-quantum safe authenticated encryption with replay protection for IoT," *Electronics*, vol. 14, no. 13, Art. no. 2668 (2025).

[2] J. Kaur, A. C. Canto, M. M. Kermani, and R. Azarderakhsh, "A survey on the implementations, attacks, and countermeasures of the NIST lightweight cryptography standard: Ascon," *ACM Comput. Surv.*, vol. 58, no. 1, pp. 1–16 (2025).

[3] A. N. Zaheer, M. Farhan, M. Rehan Naeem and M. M. Alnfiai, "Quantum-Resilient Cryptographic Frameworks: Design and Analysis of Post-Quantum Algorithms for Secure and Efficient Edge-Assisted IoT Ecosystems in Consumer Electronics Devices," in *IEEE Transactions on Consumer Electronics,* vol. 71, no. 4, pp. 11258-11268 (Nov. 2025), doi: 10.1109/TCE.2025.3619556.

[4] K. Tran-Hoang and H. Nakajo, "Kyress: A secure, scalable, and resource-efficient CRYSTALS-Kyber cryptosystem for low-cost embedded devices," *J. Supercomput*., vol. 82, no. 2, Art. no. 101 (2026).

[5] G. Tasopoulos, J. Li, A. P. Fournaris, R. K. Zhao, A. Sakzad, and R. Steinfeld, "Performance evaluation of post-quantum TLS 1.3 on resource-constrained embedded systems," in *Proc. Int. Conf. Inf. Security Practice Experience (ISPEC)*, Lecture Notes Comput. Sci., vol. 13620. Cham, Switzerland: Springer, pp. 432–451 (2022).

[6] J. Señor, J. F. Paris, and P. Martínez-España, "Analysis of the NTRU post-quantum cryptographic scheme in constrained IoT edge devices," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 18778–18790 (Oct. 2022).

[7] A. Abdulrahman, H.-C. Chen, V. Hwang, M. J. Kannwischer, T. Sprenkels, and B.-Y. Yang, "Faster Kyber and Dilithium on the Cortex-M4," in *Proc. Appl. Cryptogr. Netw. Security (ACNS)*, Lecture Notes Comput. Sci., vol. 13269. Cham, Switzerland: Springer, pp. 853–871 (2022).

[8] W. -K. Lee and S. O. Hwang, "High Throughput Implementation of Post-Quantum Key Encapsulation and Decapsulation on GPU for Internet of Things Applications," in *IEEE Transactions on Services Computing,* vol. 15, no. 6, pp. 3275-3288, 1 Nov.-Dec. 2022, doi: 10.1109/TSC.2021.3103956.

[9] P. Ravi, S. Bhasin, S. S. Roy, and A. Chattopadhyay, "On exploiting message leakage in (few) NIST PQC candidates for practical message recovery and key recovery attacks," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 684–699 (2022).

[10] L. Backlund, K. Ngo, J. Pan, and R. Wikström, "Secret key recovery attack on masked implementations of CRYSTALS-Kyber," in *Proc.*

*Appl. Cryptogr. Netw. Security (ACNS)*, Lecture Notes Comput. Sci., vol. 13906. Cham, Switzerland: Springer, pp. 159–177 (2023).

[11] S. Alnahawi, J. Müller, J. Wiesmaier, and A. Heinemann, "On the state of crypto-agility," *Cryptology ePrint Archive*, Rep. 2023/487 (2023).

[12] G. Tasopoulos, C. Dimopoulos, A. P. Fournaris, R. K. Zhao, A. Sakzad, and R. Steinfeld, "Energy consumption evaluation of post-quantum TLS 1.3 for resource-constrained embedded devices," in *Proc. ACM Int. Conf. Comput. Frontiers (CF)*, pp. 366–374 (2023).

[13] M. Mamun, M. Nguyen, and M. Abdelaziz, "Enhancing IoT security: An innovative key management system for lightweight block ciphers," *Sensors*, vol. 23, no. 18, Art. no. 7678 (Sep. 2023).

[14] S. Khan, D. Basu, S. O. Hwang, and W.-K. Lee, "Securing the IoT ecosystem: ASIC-based hardware realization of ASCON lightweight cipher," *Int. J. Inf. Security*, vol. 23, no. 6, pp. 3653–3664 (Dec. 2024).

[15] M. S. Turan, K. McKay, D. Chang, L. E. Bassham, J. Kang, N. D. Waller, J. M. Kelsey, and D. Hong, "Status report on the final round of the NIST lightweight cryptography standardization process," *NIST Interagency Rep. (NISTIR)* 8454, Nat. Inst. Standards Technol., Gaithersburg, MD, USA (2023).

*Received March, 2026*