KnowledgeTrend
An International Journal

Volume 1 | Issue 1
ISSN: 3141-643X

DOI 10.5281/zenodo.22730344

Cumulative-Exposure Thresholds in Post-Quantum Migration Risk: An Occupation-Time Model with Exact Passage Laws

Tombotamunoa W. J. Lawson[1,*]

[1] Department of Mathematics, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Nigeria

[*]**Corresponding author:** tombotamunoa.lawson@iaue.edu.ng

Abstract

A Markov model that allows a vulnerable cryptographic deployment to return to a safe state can inadvertently erase risk accumulated before remediation. We formulate a cumulative-exposure threshold model for post-quantum migration analysis. A two-state continuous-time chain alternates between protected and exposed operation, but a separate, nondecreasing occupation-time variable records total exposed time. A threshold event occurs when this variable first reaches a specified budget. We derive the exact passage-time distribution as a Poisson mixture of Erlang laws, its Laplace transform, mean, variance, and a finite-horizon transform. If compromise also arrives with constant hazard per unit of exposed time, the probability of compromise before the budget is exhausted is $1 - e^{-\phi B}$*, independent of the recovery rate; recovery delays the event in calendar time without eliminating recorded exposure. An extension to finite-state operational regimes follows from the Feynman–Kac formula. Numerical values in the paper are synthetic and illustrate the mathematical mechanism rather than estimate the security of any standardized algorithm. The contribution is a testable risk-model architecture and exact benchmark for assessing migration policies when exposure cannot be reset by repair.*

Keywords:post-quantum migration; occupation time; Markov additive process; cumulative exposure; first passage; cryptographic risk.
MSC 2020: 60J27, 60J75, 68P25.

1. Introduction

Post-quantum migration is an operational process involving discovery, prioritization and replacement of vulnerable cryptographic use, rather than an instantaneous change in a mathematical hardness assumption. NIST has standardized ML-KEM, ML-DSA and SLH-DSA in FIPS 203–205 [2, 3, 4], and its migration project emphasizes discovery and cryptographic agility [5]. Shor's result explains the concern for deployed public-key systems based on factoring and discrete logarithms [1]. These facts do not give a measured failure clock for a particular post-quantum implementation.

The accompanying earlier manuscript, "A Continuous-Time Markov Chain Model for Evaluating Security Degradation in Post-Quantum Cryptographic Systems," uses recoverable security states and an absorbing failure state [8]. It gives a useful snapshot model but motivates a distinct question: what if a return to protected operation does not undo records collected or opportunities accumulated while exposed? This paper retains a continuous-time operational chain but adds an irreversible exposure

coordinate. The resulting process is not a finite-state CTMC when the exposure budget is continuous. Its first-passage law nevertheless has an exact representation in a tractable two-state case.

Ajtai's worst-case/average-case connection and Regev's learning-with-errors construction establish key mathematical foundations for lattice cryptography [9, 10]. John, Udoaka and Udoakpan discuss a group-theoretic perspective on lattice-based cryptography [11], while John and coauthors discuss lattices in quantum-era cryptography [15]. These are background on the algebraic setting, not measurements of an operational failure clock.

Other algebraic studies include solvable groups and monomial characters [12], conjugacy classes of finitely generated groups [13], nilpotent-group key exchange [14], number theory in RSA [16], and fuzzy group actions on near-ring subgroups [17]. They illustrate different mathematical objects and cryptographic contexts. None provides the transition rates or an empirical exposure threshold used in the present model; our stochastic results are derived from the assumptions below.

The modelling claim is conditional. Accumulated exposure is appropriate only when a meaningful risk quantity persists through remediation, for example previously captured material, cumulative vulnerable operating time, or a conservatively defined monitoring budget. It should not be interpreted as a cryptanalytic theorem, a claim that all attacks add linearly over time, or a forecast for ML-KEM. The threshold B and rates must be justified for a concrete deployment before decision use.

2. Model and assumptions

Let $J_t \in \{0, 1\}$ denote protected and exposed operation, respectively. Its generator, with row-vector convention, is

$$Q = \begin{pmatrix} -\lambda & \lambda \\ \mu & -\mu \end{pmatrix}, \qquad \lambda > 0, \quad \mu \geq 0. \tag{1}$$

The process starts protected: $J_0 = 0$. Define accumulated exposure and budget-passage time by

$$A_t = \int_0^t \mathbf{1}_{\{J_s=1\}}\, ds, \qquad \tau_B = \inf\{t \geq 0 : A_t \geq B\}, \qquad B > 0. \tag{2}$$

Protected intervals pause, rather than reverse, A_t. The threshold is a modelled unacceptable-exposure criterion, not necessarily a cryptographic break. If the system starts exposed, the initial protected waiting time in the results below is omitted.

An optional independent compromise clock operates only while exposed at intensity $\phi \geq 0$ per unit of exposed time. Conditional on a path, the probability of no such compromise by t is $e^{-\phi A_t}$. The clock is distinct from threshold passage: the first describes a stochastic attack event; the second describes an exposure-budget rule. No empirical value is assigned to λ, μ, B or ϕ here.

3. Exact passage law

The exposure clock runs only in state 1. Viewed on that clock, exits from state 1 form a Poisson process of rate μ. Every exit is followed by an independent protected sojourn of rate λ before exposure resumes. The initial protected sojourn is of the same law.

Theorem 1 (Poisson–Erlang representation)**.** *For $\mu \geq 0$, let $N_B \sim \text{Poisson}(\mu B)$ and let $W_0, W_1, \ldots$ be independent $\text{Exp}(\lambda)$ variables, independent of N_B. Then*

$$\tau_B \overset{d}{=} B + \sum_{k=0}^{N_B} W_k. \tag{3}$$

Consequently, for $q \geq 0$,

$$\mathbb{E}[e^{-q\tau_B}] = e^{-qB}\frac{\lambda}{\lambda+q}\exp\left[-\mu B\frac{q}{\lambda+q}\right], \tag{4}$$

and

$$\mathbb{E}[\tau_B] = B + \frac{1+\mu B}{\lambda}, \qquad \mathrm{Var}(\tau_B) = \frac{1+2\mu B}{\lambda^2}. \tag{5}$$

Proof. On the exposed-time scale, holding times in state 1 are independent $\mathrm{Exp}(\mu)$ intervals. Thus the number of completed exposed intervals before exposed time B is Poisson with mean μB. Each completed interval necessitates one protected sojourn, in addition to the initial protected sojourn. Equality at the end of an exposed interval has probability zero. This proves (3). Conditional on $N_B = n$, the sum of $n+1$ independent protected sojourns has Erlang shape $n+1$ and rate λ. Taking its Laplace transform and then the probability-generating function of N_B gives (4). Conditional variance and the law of total variance give $\mathbb{E}[(N_B+1)/\lambda^2] + \mathrm{Var}(N_B)/\lambda^2 = (1+2\mu B)/\lambda^2$; the mean follows similarly. The case $\mu = 0$ is the degenerate Poisson case. □

For $t > B$, let $F_{k,\lambda}(x) = 1 - e^{-\lambda x}\sum_{j=0}^{k-1}(\lambda x)^j/j!$ be the Erlang CDF. Conditioning in (3) yields an evaluable finite-horizon series:

$$\mathbb{P}(\tau_B \leq t) = e^{-\mu B}\sum_{n=0}^{\infty}\frac{(\mu B)^n}{n!}F_{n+1,\lambda}(t-B), \tag{6}$$

with value zero for $t \leq B$. Truncating after $n = m$ has absolute error no larger than $\mathbb{P}(N_B > m)$, a direct numerical accuracy certificate. Equation (6) is also a simulation benchmark.

Proposition 1 (Persistent attack exposure)**.** *Under the exposed-time attack clock, the probability that stochastic compromise occurs before τ_B equals $1 - e^{-\phi B}$. In particular, changing λ or μ alone does not change this probability under the stated attack-clock assumptions.*

Proof. The exposure variable increases continuously from zero to B at τ_B. Conditional survival of the independent clock along any path to threshold is $e^{-\phi A_{\tau_B}} = e^{-\phi B}$. Taking expectations proves the claim. Independence of operational transitions and the attack clock is essential. □

Remark 1. *The invariance in Proposition 1 is not a recommendation against remediation. Increasing μ lengthens the calendar time to threshold in this model, while lowering ϕ, lowering exposed-state incidence λ, or reducing the amount of material at risk can change a deployment's real risk. A finite calendar horizon also changes the comparison. If remediation destroys captured material or resets the attack process, a different model is required.*

4. Finite-horizon transform and extension

For $s \geq 0$, define $u_i(t,s) = \mathbb{E}_i[e^{-sA_t - \phi A_t}]$, starting in state i. The finite-state Feynman–Kac formula [6, 7] gives

$$\begin{pmatrix} u_0(t,s) \\ u_1(t,s) \end{pmatrix} = \exp[t\,(Q - (s+\phi)\,\mathrm{diag}(0,1))]\,\mathbf{1}. \tag{7}$$

For a constant budget B, the Laplace transform in B of joint survival from attack and threshold up to t is

$$\int_0^\infty e^{-sB}\mathbb{E}_0[e^{-\phi A_t}\mathbf{1}_{\{A_t<B\}}]\,dB = \frac{1}{s}\,\mathbf{e}_0^{\mathsf{T}}e^{t[Q-(s+\phi)\,\mathrm{diag}(0,1)]}\mathbf{1}, \qquad s > 0. \tag{8}$$

Indeed, conditional on $A_t = a$, $\int_a^\infty e^{-sB}dB = e^{-sa}/s$. The strict inequality handles the atom at $A_t = 0$ correctly for $B > 0$. Numerical Laplace inversion in B provides finite-horizon budget survival without sampling paths.

For d operational states with generator Q_d and nonnegative exposure rewards r_i, replace $\mathrm{diag}(0,1)$ by $D = \mathrm{diag}(r_1, \ldots, r_d)$ and set $A_t = \int_0^t r_{J_s} ds$. If state-dependent attack intensity is h_i, use $Q_d - sD - \mathrm{diag}(h_i)$ in (7); this is the general Markov reward formulation. The exact Poisson–Erlang representation requires the special alternating two-state assumptions and is not claimed for arbitrary Q_d.

5. Illustrative results and policy interpretation

Table 1 evaluates the exact formulas for $B = 2$ exposure units, $\lambda = 0.2$ per calendar unit, and $\phi = 0.1$ per exposure unit. These dimensionless, synthetic rates are chosen to make the calculations transparent. They are not calibrated to NIST standards or to observed attacks. The attack probability

Table 1: *Exact synthetic illustrations with $B = 2$, $\lambda = 0.2$, $\phi = 0.1$.*

μ	$\mathbb{E}[\tau_B]$	$\mathrm{Var}(\tau_B)$	$\mathbb{P}(\text{attack before } \tau_B)$	$\mathbb{E}[N_B]$
0.0	7.0	25.0	0.1813	0.0
0.1	8.0	35.0	0.1813	0.2
0.3	10.0	55.0	0.1813	0.6
0.5	12.0	75.0	0.1813	1.0

is $1 - e^{-0.2} = 0.181269\ldots$; values in the table are rounded. The invariance is a feature of holding the exposure budget and exposed-time attack intensity fixed. It isolates the difference between delaying exposure in calendar time and actually removing accumulated exposure.

For a fixed migration deadline T, the appropriate quantity is $\mathbb{P}(\tau_B \le T)$ from (6), not merely $\mathbb{E}[\tau_B]$. In deployments where confidentiality value decays or adversarial capability changes with calendar time, rates should be time dependent; Proposition 1 would then generally cease to hold. Empirical application requires: a defined asset and security objective; auditable protected/exposed state criteria; operational transition data; a defensible exposure reward and budget; and a documented attack-hazard model. Sensitivity or interval analysis should accompany uncertain inputs.

6. Limitations and conclusion

The two-state model compresses many implementation and adversary variables into a binary operating condition. Exponential sojourns, independent attack exposure, constant rates, and additive exposure may be inappropriate for specific systems. The quantity B is a governance or modelling threshold unless independently justified; it is not a proof of cryptographic failure. No measurements, algorithm break estimates, or validation on real deployments are asserted here.

The conceptual change from a recoverable-state CTMC is the irreversible exposure coordinate. Under transparent assumptions, the resulting first-passage time has an exact Poisson–Erlang representation and computable finite-horizon law. This permits a sharp question for migration policy: does a control only postpone the accumulation of risk, or does it also reduce the enduring material exposed? Further work should test the exposure proxy with deployment evidence and allow time-varying attack capability, non-exponential remediation and distinct asset classes.

Declarations

Funding: No external funding is reported. **Data availability:** No empirical dataset was used; all table entries follow the stated formulas. **Conflict of interest:** The author declares no conflict of interest.

References

[1] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

[2] National Institute of Standards and Technology. (2024). *Module-lattice-based key-encapsulation mechanism standard* (FIPS 203). https://doi.org/10.6028/NIST.FIPS.203

[3] National Institute of Standards and Technology. (2024). *Module-lattice-based digital signature standard* (FIPS 204). https://doi.org/10.6028/NIST.FIPS.204

[4] National Institute of Standards and Technology. (2024). *Stateless hash-based digital signature standard* (FIPS 205). https://doi.org/10.6028/NIST.FIPS.205

[5] National Cybersecurity Center of Excellence. (n.d.). *Migration to post-quantum cryptography*. National Institute of Standards and Technology. https://www.nccoe.nist.gov/projects/migration-post-quantum-cryptography

[6] Norris, J. R. (1997). *Markov chains*. Cambridge University Press. https://doi.org/10.1017/CBO9780511810633

[7] Bladt, M., & Nielsen, B. F. (2017). *Matrix-exponential distributions in applied probability*. Springer. https://doi.org/10.1007/978-1-4939-7049-0

[8] Lawson, T. W. J. (2026). *A continuous-time Markov chain model for evaluating security degradation in post-quantum cryptographic systems*. Manuscript supplied by the author; unpublished. [Internal predecessor, cited only for the model comparison.]

[9] Ajtai, M. (1996). Generating hard instances of lattice problems (extended abstract). In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (pp. 99–108). ACM.

[10] Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM, 56*(6), Article 34. https://arxiv.org/abs/2401.03703

[11] John, M. N., Udoaka, O. G., & Udoakpan, I. U. (2023). Group theory in lattice-based cryptography. *International Journal of Mathematics and Its Applications, 11*(4), 111–125.

[12] John, M. N., Udoaka, O. G., & Musa, A. (2023). Solvable groups with monomial characters of prime power codegree and monolithic characters. *Bulletin of Mathematics and Statistics Research, 11*(4), 98–102. https://doi.org/10.33329/bomsr.11.4.98

[13] John, M. N., Musa, A., & Udoaka, O. G. (2024). Conjugacy classes in finitely generated groups with small cancellation properties. *European Journal of Statistics and Probability, 12*(1), 1–9. https://doi.org/10.37745/ejsp.2013/vol12n119

[14] John, M. N., Udoaka, O. G., & Musa, A. (2023). Nilpotent groups in cryptographic key exchange protocol for $N \geq 1$. *Journal of Mathematical Problems, Equations and Statistics, 4*(2), 32–34. https://doi.org/10.22271/math.2023.v4.i2a.103

[15] John, M. N., Ozioma, O., Obi, P. N., Egbogho, H. E., & Udoaka, O. G. (2023). Lattices in quantum-era cryptography. *International Journal of Research Publication and Reviews, 4*(11), 2175–2179. https://doi.org/10.5281/zenodo.10207210

[16] John, M. N., Ozioma, O., Obukohwo, V., & Egbogho, H. E. (2023). Number theory in RSA encryption systems. *GPH–International Journal of Mathematics, 6*(11), 7–16. https://doi.org/10.5281/zenodo.10209900

[17] John, M. N., & Udoakpan, I. U. (2023). Fuzzy group action on an R-subgroup in a near-ring. *International Journal of Mathematics and Statistics Studies, 11*(4), 27–31. https://doi.org/10.37745/ijmss.13/vol11n42731

Journal website: knowledgetrend.com/journal