capstract:2611.00064v1 [cs.CR] 20 Nov 2026

Cover Traffic Under Exact Stock Reconciliation

Lenora S. Valech
Centre for Information Assurance, Gradenwick Polytechnic
Sheffield, United Kingdom

Abstract

Publishing the opening and closing counts of a conserved inventory reveals the aggregate number of withdrawals. We study a mechanism that protects individual withdrawals by carrying out additional ones while keeping every published count exact. In a two-tray catering model, a steward replenishes the service tray and serves doughnuts from reserve to a separate standby roster. We give a capped additive mechanism that minimizes both the required roster and each upper tail of the number of standby servings. At $\epsilon = \ln 2$ and $\delta = 10^{-6}$, if all twelve employees decline seconds, the steward must serve all twelve standby diners with probability at least 0.995905 at the minimum reserve capacity. Sampling the indicator of actual standby service at rate λ raises the exact failure parameter of the mechanism to $\lambda + (1 - \lambda)\delta$.

CCS Concepts

• Security and privacy → Privacy-preserving protocols.

Keywords

differential privacy, cover traffic, count queries, inventory reconciliation

Reference Format:
Lenora S. Valech. 2026. Cover Traffic Under Exact Stock Reconciliation. Preprint, November 20, 2026.

1 Introduction

An inventory report can disclose a private action even if the report contains no individual records. In a closed stock, anyone who knows the opening and closing counts can determine the number of withdrawals. At a catered office handoff, that number can disclose who took a second serving. Refilling the serving tray moves stock between compartments. An auditor who counts both compartments sees the same withdrawals as before.

We study a service in which the first group has already received one doughnut per person. It is then offered seconds in private. The office requires a full tray for the next group and an exact public reconciliation of the service and reserve trays. Every doughnut missing at reconciliation must have been served. The steward can meet both conditions by serving reserve doughnuts to a separate group of standby diners. A standby serving and an employee's second serving then have the same effect on the aggregate account. The amount of cover needed is greatest when the first group declines seconds.

The mechanism is related to fixed-size cover traffic. Here the items carrying cover are charged to the same physical stock as the genuine traffic. The office must have stock to restore the serving tray and people to take the additional servings. We derive separate lower bounds on these two resources, give a mechanism that attains both, and calculate the effect of inspecting the standby serving record. All released stock counts remain exact.

2 Setting

2.1 Service and reconciliation

A batch starts with K doughnuts in a service tray and B in a reserve. Each of K eligible employees makes a private choice $d_i \in \{0, 1\}$ about taking one additional doughnut from the service tray. The roster and both opening counts are public. The steward observes the choices, and $q = \sum_i d_i$ is the number of second servings. We assume a separate group of H standby diners. Each of them is available for one serving from the reserve during the reconciliation interval. Treating a serving as indivisible rules out counting a shared doughnut as more than one transaction.

The steward replaces exactly q units in the service tray and sends U reserve units to standby diners. The office publishes the closing counts of both trays. They are verified by direct inspection. Write R for the closing reserve count and W for the total number of servings made during the batch. Then

$$R = B - q - U, \qquad W = B - R = q + U.$$

The public view (K, R) is equivalent to W. Feasibility requires $0 \le U \le H$ and $q + U \le B$. A full service tray is required on every input. This requires $B \ge K$ even when the office has no privacy requirement. Any additional reserve above K is permitted.

Figure 1 shows a batch with four second servings and five standby servings. The count of nine missing doughnuts agrees with both the closing inventory and the actual number served.

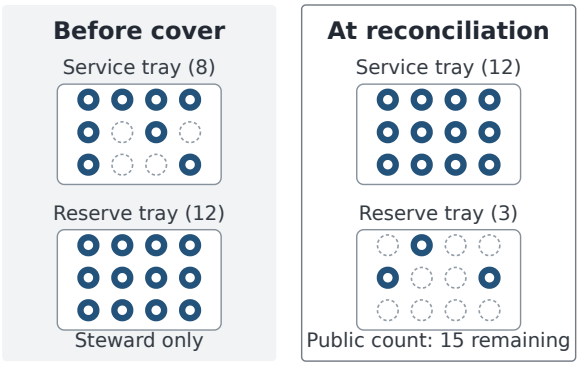


Figure 1: Inventory before and after reconciliation. Four doughnuts have already been served when the steward takes custody. The steward transfers four reserve units to the service tray and serves five from reserve. Both closing counts are public.

2.2 Privacy objective

Two inputs are adjacent if one employee changes their second-serving choice. We require (ϵ, δ)-differential privacy for the public view [4, 5]. Set $r = e^{\epsilon}$, with $\epsilon \geq 0$ and $0 \leq \delta < 1$. For every integer event S and ordered pair of adjacent inputs d, d',

$$\Pr(W \in S \mid d) \leq r \Pr(W \in S \mid d') + \delta.$$

The steward and the batch interval are trusted. The audit releases stock counts and the fixed roster size. Which standby diners are served, when they are served, and the resulting serving receipts are outside the initial view. We analyze an audit of those receipts in Section 5.

We assess the number of standby servings and the minimum standby roster that supports the guarantee. We compare mechanisms at every input, without a distribution over employee choices. An additional reserve doughnut and an additional standby diner are separate resources. A surplus in one cannot make up a shortage in the other.

3 Minimum Cover Requirement

3.1 A bound on published totals

Fix an input with $q \leq y < K$. Change refusals into second servings one at a time until the true number of seconds reaches $y + 1$. The event $W \leq y$ has probability zero at that endpoint because $W \geq q$. Let u and v be the probability of this event at two successive inputs along the path, starting from the lower true count. Privacy gives $u \leq rv + \delta$. Applying privacy to the complement in the reverse direction gives $1 - v \leq r(1 - u) + \delta$. Define

$$T(v) = \min\{rv + \delta,\ (v + r - 1 + \delta)/r,\ 1\},$$
$$G_{-1} = 0, \qquad G_j = T(G_{j-1}) \quad (j \geq 0).$$

Since T is nondecreasing, iterating backwards gives $\Pr(W \leq y \mid d) \leq G_{y-q}$. The argument accommodates mechanisms that use the full employee vector. Thresholds below q have probability zero by conservation. For $y \geq K$ we use the upper bound 1, which also applies to offices with additional reserve stock.

3.2 A matching mechanism

For $\delta > 0$, G is the cumulative distribution function (CDF) of a nonnegative integer Z. Each iteration increases G by at least δ/r unless it ends at 1. Draw Z independently of the choices and set

$$W^\star = \min(q + Z, K), \qquad U^\star = W^\star - q.$$

For $\delta = 0$, set $W^\star = K$. The steward samples the target before serving the standby group.

Theorem 1 (Minimum standby service)**.** *For any fixed employee input, $W^\star$ attains the largest feasible probability of $W \leq y$ at every threshold y under (ϵ, δ)-privacy and with unconstrained standby staffing. Consequently $U^\star$ minimizes every upper-tail probability of the standby serving count and the expected value of any nondecreasing loss on that count.*

Proof. First suppose $\delta > 0$. Write $p_j = G_j - G_{j-1}$ for $j \geq 0$, taking zero mass outside the support. The successive ratios p_j/p_{j-1} for $j \geq 1$ with $p_{j-1} > 0$ are nonincreasing. Each ratio is a secant slope of the concave map T on $[G_{j-2}, G_{j-1}]$. The intervals are ordered, and the ratio just beyond the last positive mass is zero.

Let P be the law of Z and Q that of $Z + 1$. The terms $P(j) - rQ(j)$ are positive only on a lower interval, by the ratio ordering and the zero left endpoint of Q. The reverse differences $Q(j) - rP(j)$ are positive only on an upper interval. The maximal event differences are therefore attained by a prefix and a suffix. For a prefix ending at j, the difference is $G_j - rG_{j-1} \leq \delta$. For a suffix beginning at $j + 1$, the reverse difference is $1 - G_{j-1} - r(1 - G_j) \leq \delta$. The recurrence supplies both inequalities. Thus the additive law is private before clipping, and clipping at K preserves privacy.

For $q \leq y < K$, the resulting CDF equals G_{y-q}. It is one at and above K, so it attains all the bounds. If $\delta = 0$, the recurrence stays at zero. The constant output K is private and again attains all bounds. ∎

The implementation needs at most $K - q$ CDF terms. A uniform draw on $[0, 1)$ selects the first CDF term above it, with remaining probability assigned to $W^\star = K$. For rational r and δ, the finite set of terms can be represented exactly using a common integer denominator.

3.3 Staffing and stock

Let L be the least index with $G_L = 1$, or infinity when $\delta = 0$. Among offices with $B \geq K$, the minimum standby roster is

$$H^\star = \min(K, L).$$

The mechanism suffices since $U^\star \leq H^\star$ and $W^\star \leq K \leq B$. For necessity consider a batch in which all employees decline. If $H < H^\star$, then $W \leq H$ always, in contradiction to $\Pr(W \leq H) \leq G_H < 1$. Thus a larger reserve cannot reduce staffing. Conversely, a larger standby group cannot make up a reserve shortage when all employees take seconds. For $\delta = 0$ the unique feasible private total of smallest magnitude is K, and the standby service must supply one serving for each refusal.

At $\epsilon = 0$ and $\delta > 0$, $H^\star = \min(K, \lceil 1/\delta \rceil - 1)$. With $\epsilon > 0$, while the first branch of T governs the update, $G_j = \delta(r^{j+1} - 1)/(r - 1)$. That branch ceases to govern when the preceding CDF exceeds $(1 - \delta)/(r + 1)$. For $K = 12$, $r = 2$ and $\delta = 10^{-6}$ the first branch still governs G_{11}. If every employee declines seconds, at least $1 - 4095\delta = 0.995905$ of public reconciliations must record 12 or more servings. With the minimum stock, this is exactly the probability that all twelve standby diners must be served.

4 Finite Evaluation

4.1 Baselines and checks

We used three baselines. *Fixed total* serves enough standby diners to bring the public total to K in every batch. *Uniform* uses the optimal law at $\epsilon = 0$. For the reciprocal integer values of δ considered here, its pre-clipping noise is uniform on the integers 0 through $1/\delta - 1$. *Shifted geometric* adapts a standard conserva-

tive count release [2]. The truncated law with center m gives mass proportional to $r^{-|j-m|}$ for $0 \le j \le 2m$. Its exact δ before clipping is the endpoint mass. We mix the two adjacent integer centers whose endpoint masses bracket the target δ. The resulting average of the two privacy bounds equals the requested budget. This avoids a stricter baseline arising solely from integer rounding of m.

For each tray and mechanism we enumerated the release distribution at all $K+1$ true counts. For neighboring laws P, Q, the largest forward privacy difference is $\sum_j [P(j) - rQ(j)]_+$. We computed both directions. Separately, we enumerated every subset of possible outputs for tray sizes 1 through 7, with $r \in \{1, 3/2, 2, 4\}$ and $\delta \in \{0, 1/64, 1/5, 3/7\}$. The evaluation uses exact rational arithmetic and has no sampling error.

4.2 Staffing in the absence of demand

Table 1 reports the workload on a batch in which all employees decline. With 12 employees and $\delta = 10^{-6}$, the optimum saves 0.0082 expected servings relative to a fixed total, and the roster stays at 12. Increasing the tray to 24 at the same privacy setting leaves a requirement for 24 standby diners even though only 18.41 are served in expectation. The budget-matched geometric mixture matches the optimum at the tighter setting to the precision shown. At $\delta = 1/64$ the optimal recurrence uses about 0.0049 fewer servings.

Table 1: Standby service when all employees decline seconds ($q = 0$, $r = 2$). Cells give mean servings and minimum standby roster, respectively. Fixed total attains $\delta = 0$. The other mechanisms attain the budget shown.

Capacity	δ	Fixed total	Uniform	Shifted geometric	Optimal
12	$1/64$	12.0000 / 12	10.7812 / 12	4.5508 / 10	4.5459 / 10
12	10^{-6}	12.0000 / 12	11.9999 / 12	11.9918 / 12	11.9918 / 12
24	$1/64$	24.0000 / 24	19.3125 / 24	4.5508 / 10	4.5459 / 10
24	10^{-6}	24.0000 / 24	23.9997 / 24	18.4123 / 24	18.4123 / 24
36	$1/64$	36.0000 / 36	25.5938 / 36	4.5508 / 10	4.5459 / 10
36	10^{-6}	36.0000 / 36	35.9993 / 36	18.4271 / 36	18.4271 / 36

Figure 2 gives the probability of accounting for 24 servings as the true number of second servings varies. Under the tighter budget, that total is reported in 1.49% of completely abstinent batches. When 23 employees take seconds, the office serves a standby diner with probability $1 - \delta$ to avoid recording 23. The number served on standby can differ across these two cases even when both public audits agree.

Figure 3 shows how the minimum roster changes with ϵ and δ. At $K = 36$ and $r = 2$, tightening δ from 2^{-8} to 2^{-12} increases the required roster from 14 to 22. At $\delta = 2^{-19}$, the standby roster reaches the size of the employee roster. The procurement requirement stays at 36 throughout.

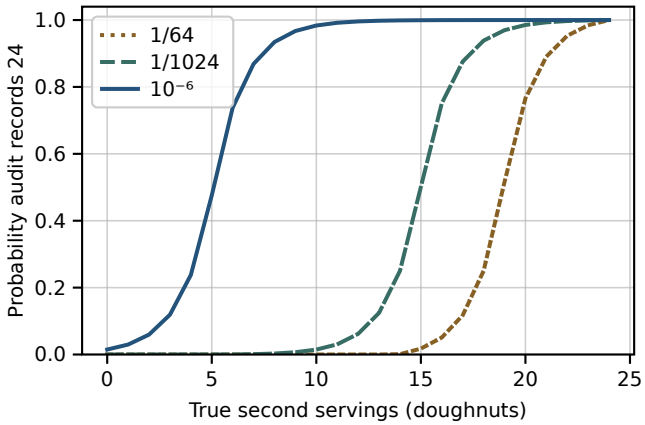


Figure 2: Probability that reconciliation records K servings for three values of δ ($K = 24$, $r = 2$). At true count q, the probability is $1 - G_{K-q-1}$, with $G_{-1} = 0$.

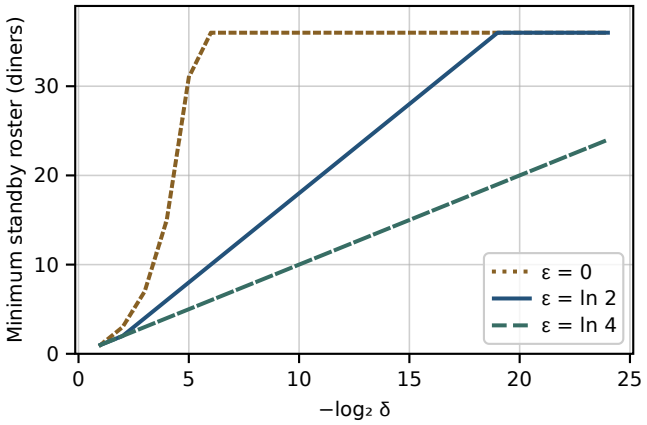


Figure 3: Minimum standby roster for a tray of capacity 36, evaluated at integer $-\log_2 \delta$.

5 Auditing the Standby Record

With the minimum reserve $B = K$, an accurate public statement of whether any standby diner was served destroys privacy. At $q = K$ the public pair consisting of W and the standby indicator is always $(K, 0)$. At $q = K - 1$ the only feasible pairs are $(K - 1, 0)$ and $(K, 1)$. The event $(K, 0)$ then requires $\delta \geq 1$. The same argument holds at any reserve capacity for the optimal mechanism, which always has $W \leq K$.

An office might disclose the standby indicator in a random sample of batches. Suppose it independently chooses each batch with probability λ and publishes a separate erasure symbol in unsampled batches. Under the optimal mechanism the exact new failure parameter at the same ϵ is

$$\delta_{\text{combined}} = \lambda + (1 - \lambda)\delta.$$

For the upper bound, restrict an arbitrary event to sampled and unsampled outcomes. The sampled branch has a maximal privacy difference of at most 1, and the unsampled branch inherits δ. For equality, order the adjacent pair from $q = K - 1$ to $q = K$. Include all sampled observations possible at $K - 1$, which are disjoint from those at K, and the unsampled observation $W = K - 1$, which occurs with probability $G_0 = \delta$ only at the first input. The calculation also holds when $\delta = 0$. We verified it on the small-tray grid above at $\lambda \in \{0, 0.01, 0.5, 1\}$ by enumerating the joint observations.

Even a one-percent sampling rate therefore imposes a failure parameter of at least 0.01. Schedules that publish the size of the fixed standby roster are compatible with the original guarantee. Payroll entries that distinguish actual standby service from attendance are a different release. Keeping the closing counts exact leaves no uncertainty about total consumption to absorb that disclosure.

6 Related Work and Scope

Fixed-rate anonymous communication uses dummy transmissions to make observed traffic less dependent on actual demand. Loopix uses cover packets at clients and service providers [7]. Our setting has a fixed interval and a public volume rather than a packet trace. Generating the volume requires both stock and a recipient for each cover serving. The signed count mechanisms in [6] allow outputs on either side of the truth, whereas an audited serving total cannot fall below the number already served. Case, Honaker, and Movahedi study nonnegative noise for conservative releases [2]. Xiao et al. treat positive bounded noise subject to general moment and support constraints [8]. Our threshold bound starts at the neighboring count where the event first becomes physically impossible. Its binary-event inequalities also arise in differentially private testing [1, 3].

The evaluation concerns counts and staffing in a single batch. It does not model diner availability or cover-service duration. The private interval must be long enough for any staffing realization, and an observer who sees its duration has a larger transcript unless the duration is fixed. Multiple batches involving the same employee require a joint privacy analysis. Stock reconciliation certifies that the servings occurred. Whether the standby roster actually reports for duty is an operational assumption.

7 Conclusion

A truthful, public inventory can conceal individual demand if part of the demand is assigned by the mechanism. In the minimum-stock office with pure differential privacy, declining a second serving sends one doughnut to the standby roster. The public account records the same number of servings on a day when every employee declines as on a day when every employee accepts.

References

[1] Jordan Awan and Aleksandra Slavković. 2018. Differentially Private Uniformly Most Powerful Tests for Binomial Data. Advances in Neural Information Processing Systems 31. https://proceedings.neurips.cc/paper/2018/hash/296472c9542ad4d4788d543508116cbc-Abstract.html

[2] Benjamin M. Case, James Honaker, and Mahnush Movahedi. 2021. The Privacy-preserving Padding Problem: Non-negative Mechanisms for Conservative Answers with Differential Privacy. arXiv:2110.08177.

[3] Jinshuo Dong, Aaron Roth, and Weijie J. Su. 2022. Gaussian Differential Privacy. *Journal of the Royal Statistical Society Series B: Statistical Methodology* 84 , 1 (2022), 3–37. https://doi.org/10.1111/rssb.12454

[4] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. 2006. Calibrating Noise to Sensitivity in Private Data Analysis. In *Theory of Cryptography Conference*. 265–284. https://doi.org/10.1007/11681878_14

[5] Cynthia Dwork and Aaron Roth. 2014. The Algorithmic Foundations of Differential Privacy. *Foundations and Trends in Theoretical Computer Science* 9 , 3–4 (2014), 211–407. https://doi.org/10.1561/0400000042

[6] Arpita Ghosh, Tim Roughgarden, and Mukund Sundararajan. 2012. Universally Utility-Maximizing Privacy Mechanisms. *SIAM Journal on Computing* 41 , 6 (2012), 1673–1693. https://doi.org/10.1137/09076828X

[7] Ania M. Piotrowska, Jamie Hayes, Tariq Elahi, Sebastian Meiser, and George Danezis. 2017. The Loopix Anonymity System. In *26th USENIX Security Symposium*. 1199–1216.

[8] Hanshen Xiao, Jun Wan, Elaine Shi, and Srinivas Devadas. 2025. One-Sided Bounded Noise: Theory, Optimization Algorithms and Applications. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 4214–4228. https://doi.org/10.1145/3719027.3765110