Private Receipt Audits for Closed Exchanges

Elina V. Tervaluoto
Department of Computing, Kivisalmi Institute of Technology
Turku, Finland
elina.tervaluoto@kivisalmi.example

Moussa L. N'Diémé
Centre for Applied Cryptography, Sendaal Institute
Saint-Louis, Senegal

Tereza Valdrenová
Laboratory for Protocol Design, Vilar de Anse Research Institute
Braga, Portugal

João F. Alvaredo
Laboratory for Protocol Design, Vilar de Anse Research Institute
Braga, Portugal

capstract:2611.00031v1 [cs.CR] 17 Nov 2026

Abstract

A closed exchange can permit private transfers while requiring public assurance that each member sent and acknowledged one item. Receipt counts alone leave the number of objects undetermined. We give a zero-knowledge audit over a registrar-committed transcript that checks sender and recipient coverage, validates custody histories and optionally attests to a lower bound on distinct items. Under a closed inventory, the distinct-item count equals the number of members who still hold their acknowledged item at cutoff. The same coverage policy certified all 32 deliveries in each of two gift-exchange enactments, although the second exchange used a single framed print and ended with the print in the possession of its original owner. On one CPU core a 32-record proof takes a median of 638 ms to generate and 3.7 ms to verify. The proof is 192 bytes. We characterize disclosure from the bound itself and distinguish evidence of physical receipt from evidence of continued possession.

CCS Concepts

• Security and privacy → Cryptographic protocols; • Security and privacy → Privacy-preserving protocols.

Keywords

zero knowledge, private audits, custody, receipt coverage, gift exchange

Reference Format:
Elina V. Tervaluoto, Moussa L. N'Diémé, Tereza Valdrenová, and João F. Alvaredo. 2026. Private Receipt Audits for Closed Exchanges. Preprint, November 17, 2026.

1 Introduction

In a conventional exchange, 32 acknowledgments are taken to mean that 32 people were given something and still have it. A recipient may hand on the same article, at which point the next acknowledgment can also be accurate. In a group that conceals giver-recipient pairings, a public custody register would resolve the ambiguity at the expense of disclosing the pairings.

We consider a fixed roster, an authenticated registrar and a closing time. Each member must give once and acknowledge once. An acknowledgment remains in the log after an onward transfer. A ceremony in which every parcel must be submitted before any can be collected is a different protocol.

We commit to the registrar's log and prove a predicate about that commitment. The resulting announcement can be checked by an auditor who has no record of the individual handovers. In a rehearsal with 32 participants, the same receipt predicate accepts a conventional exchange and an exchange in which a framed print is acknowledged and wrapped again at every handover except the last. At cutoff the original owner has the print. Every other participant's receipt is still in force.

We specify the audit interface in Section 3, give the relation and security properties in Section 4 and Section 5, and measure computation separately from the two physical enactments in Section 6.

2 Related Work

Public verification of private records follows a line from interactive zero knowledge [10] to general circuit verification [12, 18]. We recompute a Merkle commitment [15] inside the proof using a field-native hash [11]. General-purpose arguments based on discrete logarithms [4, 5] offer different setup and verification tradeoffs. Our benchmark assumes a circuit-specific common reference string.

Early anonymous payment schemes separated validity from knowledge of the payer [7]. Anonymous credentials allow holders to prove properties of credentials without revealing identity [6]. Distributed e-cash prevents a hidden unit of value from being spent twice [2, 16]. A lawful onward gift has a second transfer. The audit rules out simultaneous custody claims while counting the whole succession as one article.

We route witness rows using a permutation network [22]. Unlike a comparison-based sorting network [1], this uses switch settings supplied by the prover. We considered statistically hiding commitments [19] and chose salted hashing for smaller in-circuit cost at the price of a stronger hash model.

The separation of a transferred article from the social obligations that accompany it has a long history in studies of exchange [14, 23]. We require neither a price nor a judgment about the adequacy of the thanks. Ortega Selván and Bjerkvoll [17] records the disappearance of parcel-to-object correspondences when a group

reuses its gift envelopes. Halden and Osei-Danso [13] identifies the same issue when an exchange opens early returns before distribution closes. Their logs record entry and exit at the exchange desk. Our unit is a directed handover that has its own acknowledgment. Satō and Vilaverde-Mora [20] treats initial enrollment as a separate physical operation, which permits identity to persist after a wrapper is replaced.

3 Exchange and Audit Model

3.1 Participants and objects

An edition has an identifier e, an ordered roster of n members and exactly n authenticated handovers. Roster slots are integers in $[0, n-1]$ and are private in the audit. At opening a registrar enrolls each eligible object with a uniformly sampled unique 96-bit tag x and an initial custodian $o(x)$. A tag identifies the article inside the parcel. The wrapper and card can be replaced without enrollment.

The registrar appends (t, s_t, r_t, x_t, o_t) after checking custody and authenticating the recipient's acknowledgment. The ordinal t starts at zero and resolves events within the same wall-clock interval. The giver and recipient slots are s_t and r_t; x_t is the tag and o_t its initial custodian. The audit trusts the registrar's intake checks. Participant signatures are kept off the public transcript.

Transfers stay inside the roster until the register closes. Rewrapping does not change custody. An onward transfer between slots must appear in the log before cutoff to affect the audit.

3.2 Statements and audiences

The verifier receives a registrar-signed header with e, n, the roster version, a circuit identifier, the policy and the log commitment R. The edition announcement specifies the roster version and eligible verification key. The registrar supplies the witness and retains the history. A member knows the two events in which they participated and whatever they saw at the site.

A coverage statement, denoted C, requires one sent and one acknowledged transfer per member and admissible custody. For the retention variant C(k), the organizer also chooses an integer bound k and asks the proof to establish at least k distinct articles among the handovers. The ordinary C policy is C(1); our benchmark includes a smaller specialization that checks custody and coverage and omits the distinct count. The organizer fixes the public bound in the edition announcement before enrollment. Proofs for the same edition never answer a sequence of alternative bounds. Exact counts appear in this paper only for designated enactments and simulated logs.

A member may hold multiple objects at cutoff. Ownership of an article brought but never received contributes nothing to this audit.

4 Audit Relation

4.1 Binding the register

The registrar samples a fresh 128-bit salt ρ_t per record. Let H_{row} and H_{node} denote disjoint domains of a Poseidon sponge. In the implementation each input field occupies a canonical field slot. The leaf sponge absorbs all row fields in one width-nine permutation. The internal-node hash uses width three. Leaves bind all the fields that can affect acceptance. For a complete binary tree the commitment is

$$\begin{aligned} L_t &= H_{\mathrm{row}}(e, t, s_t, r_t, x_t, o_t, \rho_t), \\ R &= \mathrm{Merkle}_{H_{\mathrm{node}}}(L_0, \dots, L_{n-1}). \end{aligned} \tag{1}$$

Our circuits use powers of two for n. Partial ceremonies are ineligible. The authenticated header specifies the number of leaves and the expected edition. Changing a leaf position changes its ordinal as well as its path to the root. The proof relation evaluates Eq. (1) in chronological order before applying any permutation.

4.2 Coverage and custody

Two independent checked permutations route the sender and recipient columns to the public sequence $0, \dots, n-1$. This excludes duplicates and missing slots. For every row $s_t \trianglelefteq r_t$. A third network routes entire rows into ascending order on (x_t, t). The key fits well below the field modulus. A strictly increasing order test compares the routed adjacent keys. After permutation there is one consecutive run per distinct article. Start bits b_j, indexed in this sorted array, are given by

$$b_0 = 1, \quad b_j = [x'_j \neq x'_{j-1}] \quad (j > 0), \qquad D = \sum_{j=0}^{n-1} b_j. \tag{2}$$

A prime denotes the routed field. At a run start the sender must match o'_j. Otherwise the sender must match the preceding recipient and the enrollment slot must agree with the preceding enrollment slot. The relation enforces both alternatives on the same permutation:

$$\begin{aligned} 0 &= b_j(s'_j - o'_j) + (1 - b_j)(s'_j - r'_{j-1}), \\ 0 &= (1 - b_j)(o'_j - o'_{j-1}). \end{aligned} \tag{3}$$

For row zero the preceding fields are arbitrary constants and the relation fixes $b_0 = 1$. No count wraps in the field since $D \leq n$. The rule for C(k) uses an unsigned comparison of D with k. Algorithm 1 gives the corresponding plaintext checker.

Algorithm 1 Reference audit for a committed, chronological register

Input: edition e, root R, bound k, chronological rows **and** salts W
if $\mathrm{Commit}(e, W) \neq R$ **then**
  return reject
end if
if sender **or** recipient slots fail coverage **then**
  return reject
end if
$U \leftarrow \mathrm{Sort}(W,\ (x, t))$
$D \leftarrow 0$
for each row (t, s, r, x, o) **in** U **do**
  if the row starts an object run **then**
    $h \leftarrow o$
    $D \leftarrow D + 1$
  end if
  if $s \neq h$ **or** $s = r$ **then**
    return reject
  end if
  if o differs from the first enrollment slot **in** its run **then**
    return reject
  end if
  $h \leftarrow r$
end for
return $D \geq k$

4.3 Retention

The recipient of an object's last entry holds it at cutoff because the inventory is closed. Two objects cannot have the same last recipient, since that member would have acknowledged twice. An earlier recipient cannot get the same object back without a second acknowledgment. Thus the last entry of each object identifies one member who still holds their acknowledged article, and these entries exhaust such members. Write K for their number. Under C,

$$K = D. \tag{4}$$

The equality holds even if $n - 1$ members start with nothing. An inventory count at cutoff can exceed K because it includes articles that never moved.

An organizer who can impose a maximum of q handovers per article obtains $K \geq \lceil n/q \rceil$. The bound is tight by segmenting the edges of one directed cycle of recipients into consecutive blocks of length at most q (Appendix A). The exact minima are plotted in Figure 1. With $q = 1$, the first acknowledgment ends the admissible custody history for each gift. With no cap and one object, the only admissible history that meets coverage returns the object to its initial custodian. The orbit includes every member because all transfers in the committed log refer to the same object.

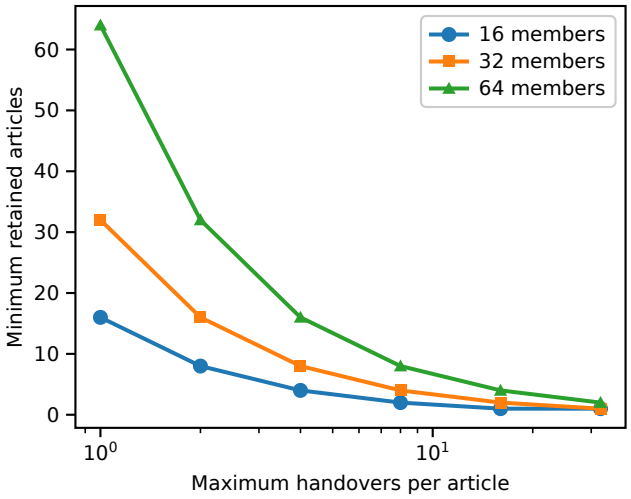


Figure 1: Minimum number of acknowledged articles still held at cutoff under a per-article handover cap. Exact combinatorial bounds.

5 Security and Disclosure

5.1 Integrity

Under knowledge soundness an accepted proof yields rows and switch settings satisfying the relation. If these rows differ from the committed register, the two tree computations have a first divergence beneath a common node, giving a hash collision. Conversely, a valid register admits switch settings for all prescribed routings. Appendix A proves the equivalence between the sorted checks and the chronological custody conditions.

The claim depends on the registrar's intake and the authoritative final header. A signature authenticates the header [3]. It cannot give independent evidence that a handover occurred. Verifiers check the header against the one published copy for the edition. The benchmark in Section 6 starts after that check.

5.2 Privacy

In the common reference string model the simulated proof reveals no information about the witness beyond the statement. For hiding of the root itself we model the domain-separated hashes as random oracles. For fixed public fields and outcome, unopened salted leaves can be replaced by uniform oracle outputs except when the observer queries an honest salt or finds a collision. Without side information about salts, the chance of a salt hit in Q queries is at most $nQ/2^{128}$. Applied to Poseidon this is a modeling assumption.

Acceptance at $k = n$ already reveals that every recipient still holds the article in their receipt. The order, pairing and descriptions are private conditional on that fact. The organizer fixes one bound because a series of decisions at different bounds could determine the exact count. A missing proof alone does not establish that a bound failed.

Two recipients who recognize the same repair to a corner of the frame can infer equality without the transcript [21]. Privacy

excludes direct observation and disclosure by the registrar. Hiding membership in the audit itself would require an additional authentication mechanism, such as group signatures [8].

6 Evaluation

6.1 Two 32-member exchanges

In both enactments 32 participants handed something to the next slot around an agreed cycle. In the first, each gave a separate framed print held at opening. In the second, there was one framed print, enrolled to the first sender. Each recipient acknowledged it before moving it to a wrapping station. The final recipient was the first sender. The registrar checked the tag behind the frame backing at every handover and at cutoff. The carton and paper were replaced 31 times, so there were as many parcels as acknowledgments.

The 64 enacted handovers form two logs at the attainable extremes of Eq. (4). Participants read the same receipt acknowledgment in both conditions. We tracked serial identity and custody rather than asking the recipients to judge resemblance. Two additional logs assign different tags to four-edge or eight-edge segments of the same cycle. Table 1 gives the results for all four logs.

Table 1: Audit results for two enacted and two constructed editions. Each log has 32 sent and 32 acknowledged transfers. The C(k) columns are counterfactual policy tests.

Register	Distinct D	Retained K	Retained article-events	C(1)	C(8)	C(32)
Individually supplied	32	32	528	Pass	Pass	Pass
Four handovers per article	8	8	144	Pass	Pass	Fail
Eight handovers per article	4	4	80	Pass	Fail	Fail
One circulating article	1	1	32	Pass	Fail	Fail

The column of retained article-events sums the number of recipients holding their acknowledged articles immediately after each handover. At step m in a log with q handovers per article, the count is $\lceil m/q \rceil$. For the single print each new acknowledgment replaces the previous holder's contribution, so the sum is 32. With individual articles the count rises at every step, giving 528. These are counts weighted by event. Weighting by elapsed minutes would make them depend on time spent rewrapping.

The slot sequence alone cannot distinguish the two enactments. Nor can the opening and closing position establish that the one print moved at all. Its entire change in location is in the witness.

6.2 Implementation and measurement

We used Groth16 over BLS12-381. The full C(k) circuit checks $k = n/2$ in timed runs. An intact-custody specialization omits the sum in Eq. (2) and the bound comparison. A custody-free baseline commits to the same rows and checks the slots but drops the ordering and custody calculation.

Each benchmark seed chooses a random recipient cycle, a segmentation conditional on $D \geq n/2$, and fresh salts. Paired runs use the same log. The one-print enactment is verified against C(1) outside this sample.

We pinned one core of a Ryzen 7 7700 (32 GiB DDR5, turbo disabled). Prover time spans witness construction through serialization. Verification spans proof decoding through the pairing check. The two compressed first-group elements and one second-group element total 192 bytes. Latencies exclude key generation, key loading and header checks. We visit 48 independently seeded, randomized logs per size and circuit in 12 blocks after six untimed proofs. Intervals use 10,000 block-bootstrap draws [9].

6.3 Proving and verification costs

Figure 2 shows the timing curves; Table 2 gives their medians along with circuit sizes. At $n = 32$ full generation takes 638 ms (95% interval 622 to 654 ms), while the intact-custody coverage specialization takes 635 ms (619 to 651 ms). The custody-free audit takes 428 ms (417 to 439 ms). The median within-log difference of full minus intact-custody generation is 3 ms (-2 to 8 ms). The smaller comparison is the relevant one if the registrar has already implemented the custody predicate. A verifier checks a bounded number of public inputs and a three-element proof at each size. Observed verification medians span 3.6 to 3.8 ms for the full circuit.

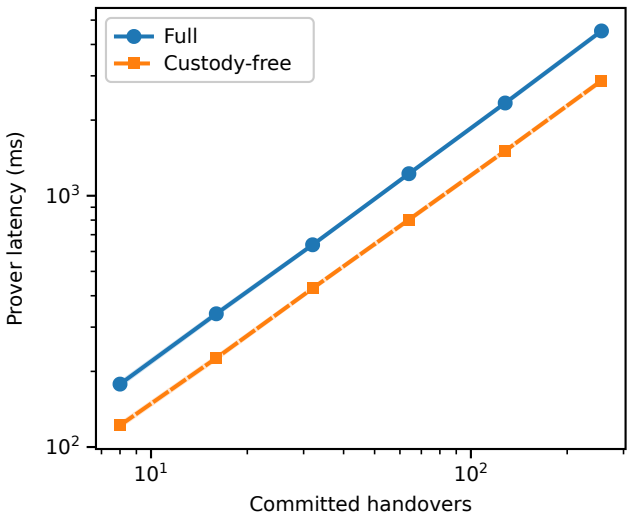


Figure 2: Prover latency by register size. Points are medians over 48 logs per circuit and size. Bands show central 95% block-bootstrap intervals.

Table 2: Benchmark medians and multiplication-constraint counts. Columns labeled C use intact custody; the last column omits custody.

Rows	Full constraints	C constraints	No-custody constraints	Full prove (ms)	C prove (ms)	No-custody prove (ms)
8	9,808	9,787	6,094	178	177	122
16	20,562	20,537	12,502	339	338	226
32	43,306	43,277	25,590	638	635	428
64	91,418	91,385	52,270	1,224	1,217	803
128	192,994	192,957	106,670	2,339	2,327	1,509
256	406,770	406,729	217,550	4,527	4,511	2,870

We measured peak resident memory in one additional fresh process per seed. Figure 3 includes key and witness allocations. The full 256-row circuit is the only one whose median exceeds 256 MiB.

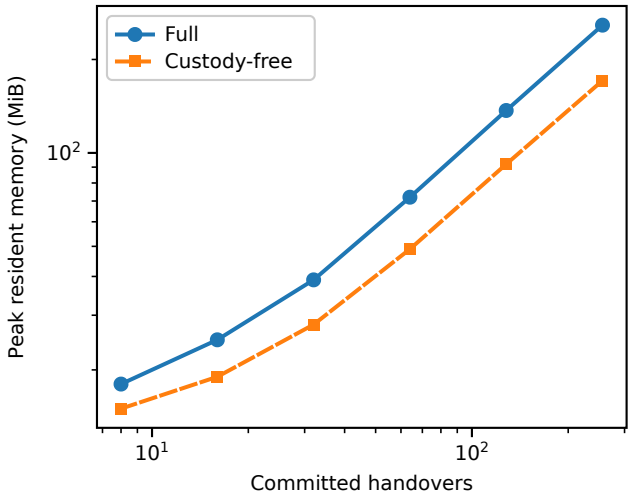


Figure 3: Peak process resident memory during proof generation, including the proving key. Points are medians from 48 fresh processes per size and circuit.

On 1,000 valid 32-row histories with $D < 32$, we tested one repeated recipient, one changed initial custodian on the first row and one bound of $D + 1$. Each change to a row received a recomputed commitment. The plaintext and circuit checkers accepted all 1,000 base histories and rejected all 3,000 invalid variants.

7 Limitations

If an interchangeable mat is replaced, a registrar must decide whether identity persists. We tracked intact articles. Two visually identical framed prints count twice when enrolled and transferred separately.

Retention is defined at cutoff. A recipient can give away the print while leaving the building. Extending the window requires a new closing transcript, and overlapping audits would disclose more about the path. We have analyzed one fixed edition.

The enactments test trace feasibility only. Willingness to acknowledge the same article on successive occasions and time spent inspecting or rewrapping it were outside the measurement plan.

8 Conclusion

For a group that meets once and certifies an exchange at the end, the last acknowledgment for each article identifies the current holder. If the object goes back to the first giver, the last receipt still contributes one to retention, even if the print goes back on the hook it occupied that morning. An organizer setting the bound for the next edition has to decide whether that outcome counts as a completed exchange.

A Proof Details

A.1 Equivalence to sequential custody

Sorting one tag by ordinal gives its original order within the full transcript. At the head the sender is the initial custodian by Eq. (3). After event i the recipient is the only custodian, so the transition at $i + 1$ must begin with that slot. Interleaved events for other tags have no effect. An induction proves equivalence to sequential custody. Every routing switch preserves both complete records by choosing either identity or swap. The two coverage networks likewise preserve the multiplicities of their respective input columns.

A.2 Achieving the retention bound

Traverse a fixed n-cycle in order, cutting its edges into blocks of size q with at most one shorter block. Enroll each block's article to the sender of its first edge. All remaining senders in that block receive its article immediately before their turn. This uses $\lceil n/q \rceil$ articles. Fewer articles would supply fewer than n transfers. The case $q \geq n$ gives a single article returning to its initial custodian.

B Encoding and Instrumentation

The canonical fields of a row hash are the edition, ordinal, sender, recipient, tag, opening custodian and salt. The row domain separator occupies a capacity slot. Tags are 96-bit integers. Salts are generated as 128-bit integers and admitted as field elements. The circuit range-checks tags, slot identifiers and the public bound. The ordinal is fixed by leaf position. The routed ordering test decomposes each adjacent key difference minus one in a

width smaller than the modulus by more than the largest key. A negative difference has no witness in that width. Equality of adjacent tags uses a zero test with an inverse witness.

For the paired interval we subtract latencies per log, then resample 12 blocks of four pairs. We round the plotted intervals to milliseconds. Size and verification use the canonical compressed encoding of the proof. The reference string is generated separately for each size and relation.

Acknowledgments

We thank the members of the two rehearsal exchanges and Marta E. Lubień for checking the closed-inventory argument.

References

[1] Kenneth E. Batcher. 1968. Sorting Networks and Their Applications. In *AFIPS Spring Joint Computer Conference*..

[2] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. 2014. Zerocash: Decentralized Anonymous Payments from Bitcoin. In *IEEE Symposium on Security and Privacy*..

[3] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. 2012. High-speed High-security Signatures. *Journal of Cryptographic Engineering* 2 (2012), 77–89.

[4] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth, and Christophe Petit. 2016. Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting. In *EUROCRYPT*..

[5] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. 2018. Bulletproofs: Short Proofs for Confidential Transactions and More. In *IEEE Symposium on Security and Privacy*..

[6] Jan Camenisch and Anna Lysyanskaya. 2001. An Efficient System for Nontransferable Anonymous Credentials with Optional Anonymity Revocation. In *EUROCRYPT*..

[7] David Chaum. 1983. Blind Signatures for Untraceable Payments. In *Advances in Cryptology: Proceedings of Crypto 82*..

[8] David Chaum and Eugène van Heyst. 1991. Group Signatures. In *EUROCRYPT*..

[9] Bradley Efron and Robert J. Tibshirani. 1993. *An Introduction to the Bootstrap*. Chapman and Hall.

[10] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. 1989. The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing* 18 , 1 (1989), 186–208.

[11] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. 2021. Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. In *USENIX Security Symposium*. 519–535.

[12] Jens Groth. 2016. On the Size of Pairing-Based Non-interactive Arguments. In *EUROCRYPT*..

[13] Sivert B. Halden and Beatrice Osei-Danso. 2022. Overlapping Returns and Distributions in Closed Exchange Registers. In *Workshop on Institutional Records and Audit*..

[14] Marcel Mauss. 1990. *The Gift: The Form and Reason for Exchange in Archaic Societies*. Routledge.

[15] Ralph C. Merkle. 1988. A Digital Signature Based on a Conventional Encryption Function. In *Advances in Cryptology: CRYPTO '87*..

[16] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. 2013. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In *IEEE Symposium on Security and Privacy*..

[17] Lucía Ortega Selván and Synnøve R. Bjerkvoll. 2019. Envelope Reuse and Unit Counts in Rotating Parcel Exchanges. *Journal of Documentary Practice* 8 , 2 (2019), 64–81.

[18] Bryan Parno, Jon Howell, Craig Gentry, and Mariana Raykova. 2013. Pinocchio: Nearly Practical Verifiable Computation. In *IEEE Symposium on Security and Privacy*..

[19] Torben Pryds Pedersen. 1992. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In *Advances in Cryptology: CRYPTO '91*..

[20] Akiho Satō and Iván Vilaverde-Mora. 2024. Object Enrollment in Short-Lived Custody Systems. *Transactions on Applied Recordkeeping* 5 (2024), 103–119.

[21] Claude E. Shannon. 1949. Communication Theory of Secrecy Systems. *Bell System Technical Journal* 28 , 4 (1949), 656–715.

[22] Abraham Waksman. 1968. A Permutation Network. *Journal of the ACM* 15 , 1 (1968), 159–163.

[23] Viviana A. Zelizer. 1994. *The Social Meaning of Money*. Basic Books.