Karlsruhe Institute of Technology

KASTEL

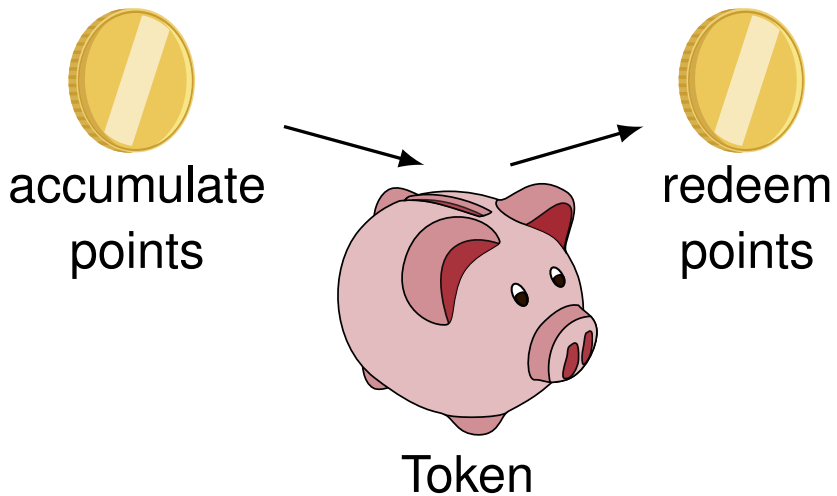
BABL

Black-Box Accumulation Based on Lattices

S.H. Faller, P. Baumer, M. Klooß, A. Koch, A. Ottenhues, M. Raiber | 14. Dec 2021

What ist Black-Box Accumulation (BBA)?

- Cyptographic protocol for point transfer
- Users can charge their token with points
- Points can be redeemed later
- Introduced by Jager and Rupp [JR16]. Several improvements: [Har+17; Hof+20; Bob+20; Blo+19].



BBA Scenarios

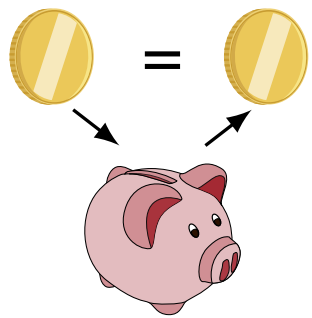
Possible scenarios:

- Prepayment systems (e.g. in public transport)
- Loyalty programs
- Reputation systems

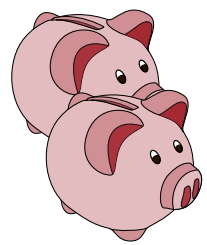
Important BBA Properties

Privacy:

Balance-binding:



Double-Spending-Detection:



Core idea: Updating tokens

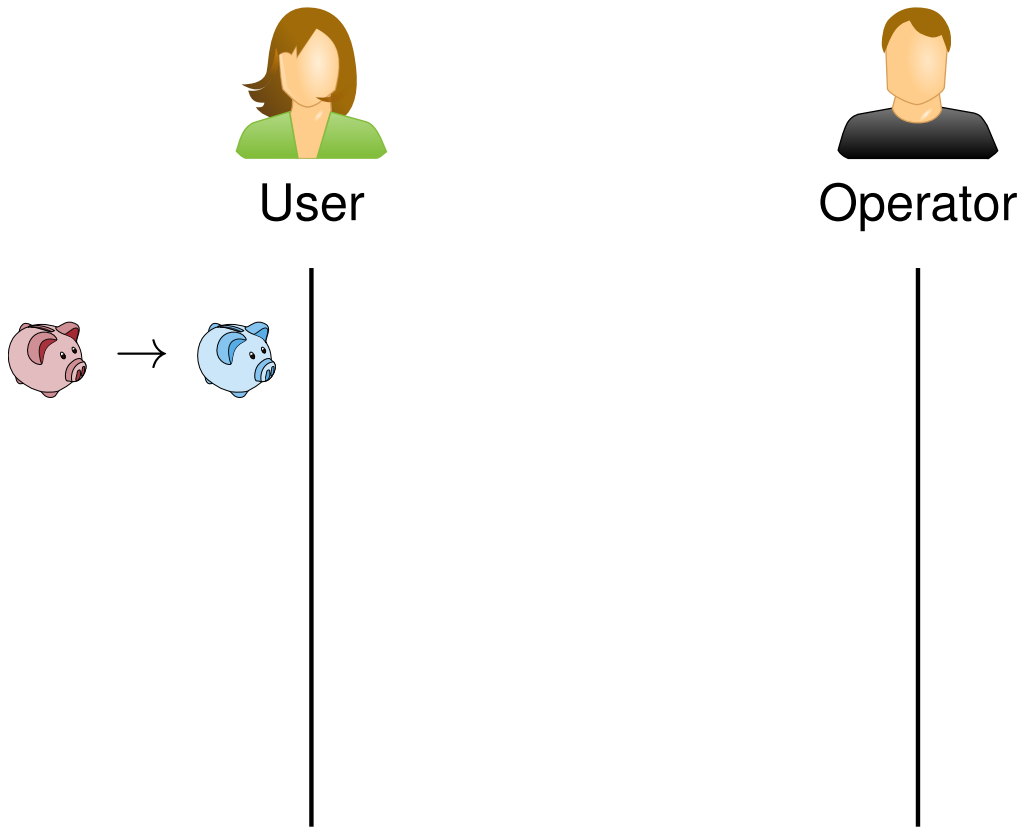


Figure: Sketch of the *Update*-protocol, graphics by M. Nagel

Core idea: Updating tokens

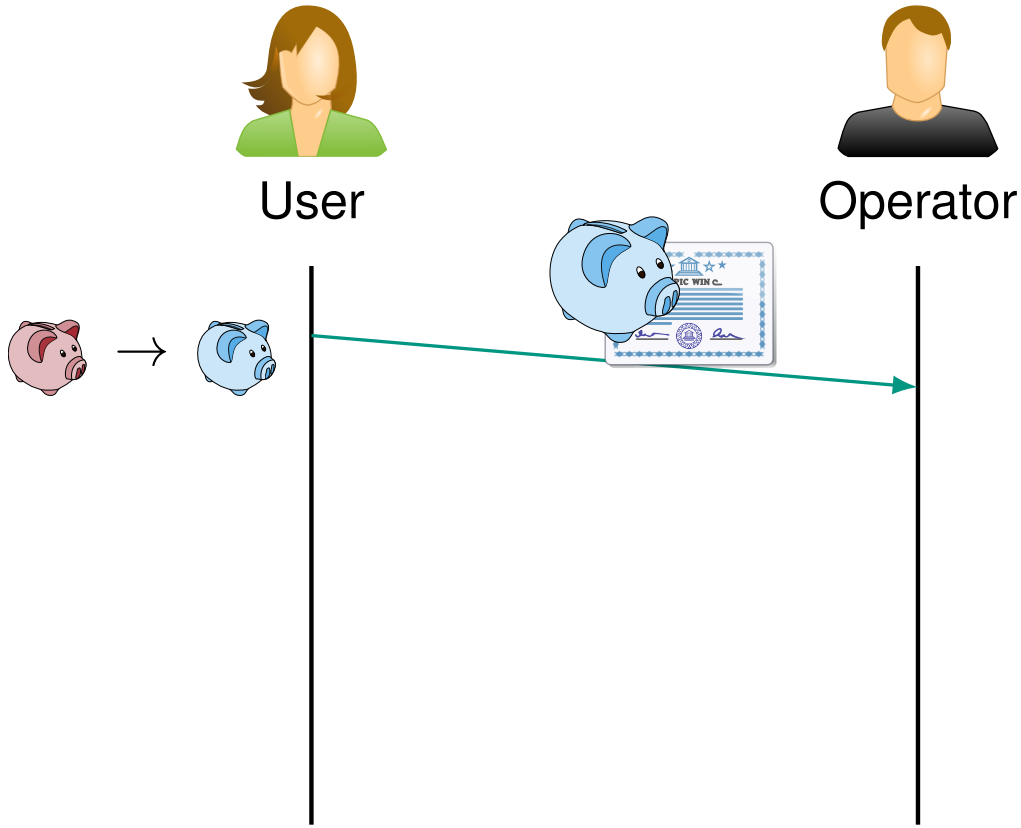


Figure: Sketch of the *Update*-protocol, graphics by M. Nagel

Core idea: Updating tokens

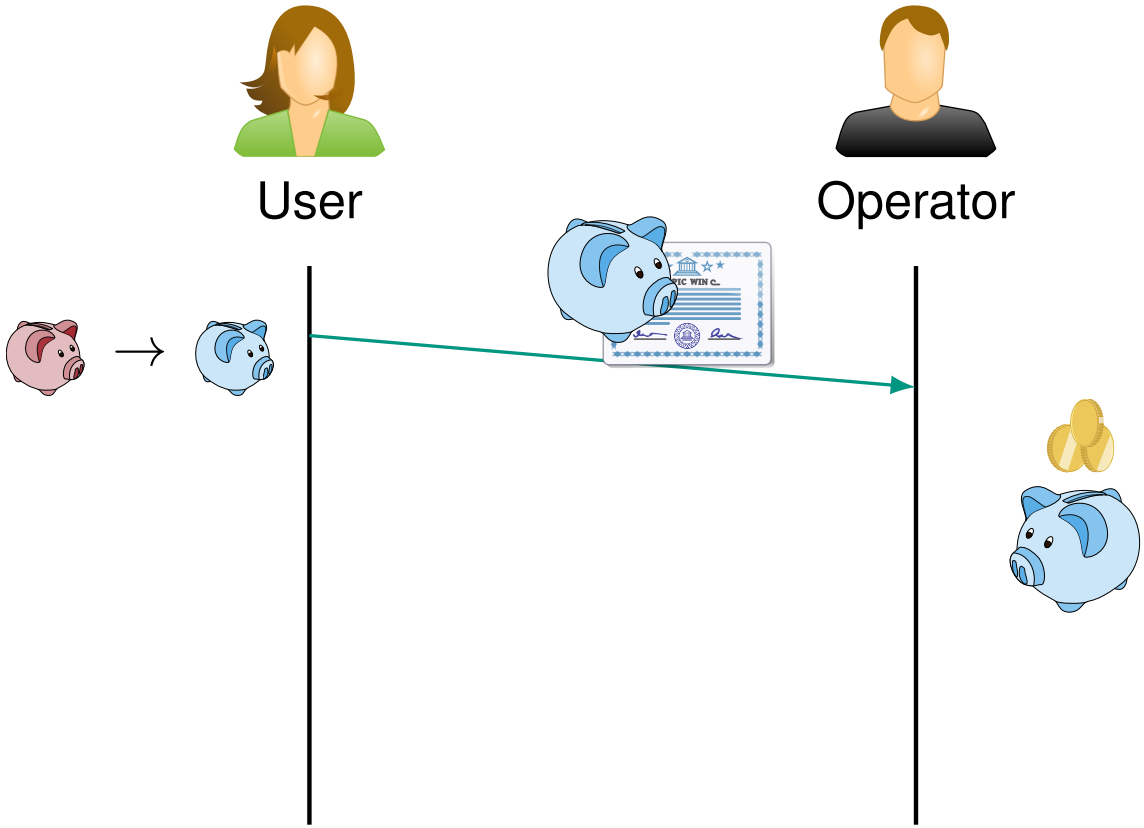


Figure: Sketch of the *Update*-protocol, graphics by M. Nagel

Core idea: Updating tokens

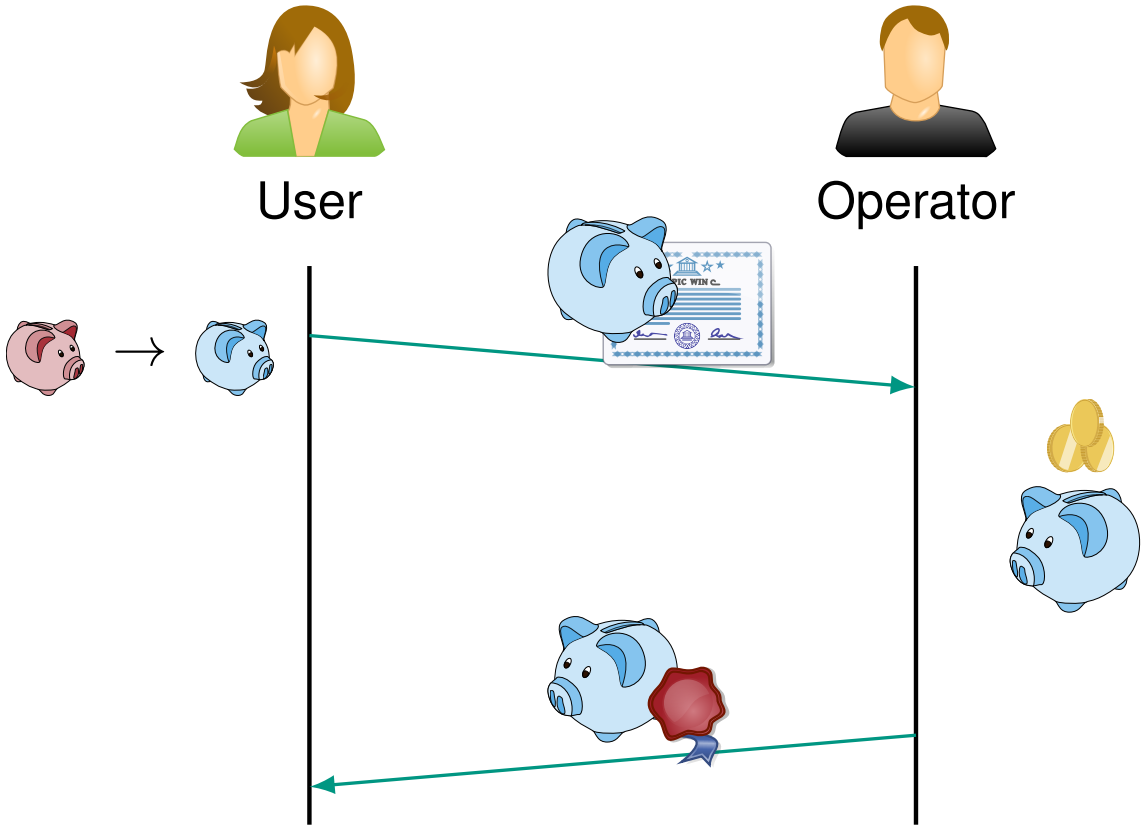


Figure: Sketch of the *Update*-protocol, graphics by M. Nagel

Motivation

- All prior work on BBA relied on classical hardness assumptions
- Is a lattice-based construction of BBA feasible?
- How efficient will the construction be?

Double-Spending Tags

Same idea as in [Har+17]. Informally:

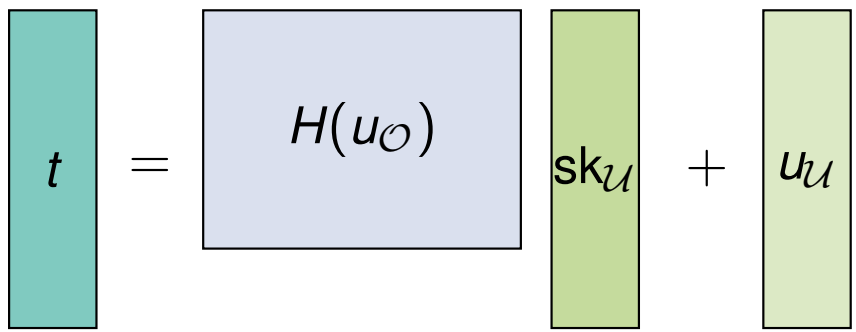
$$t = \mathsf{sk}_{\mathcal{U}} \cdot u_{\mathcal{O}} + u_{\mathcal{U}},$$

$u_{\mathcal{U}}$ was fixed when token is issued
$u_{\mathcal{O}}$ is drawn when token is used.
If same token is used again:

$$t' = \mathsf{sk}_{\mathcal{U}} \cdot u'_{\mathcal{O}} + u_{\mathcal{U}}$$

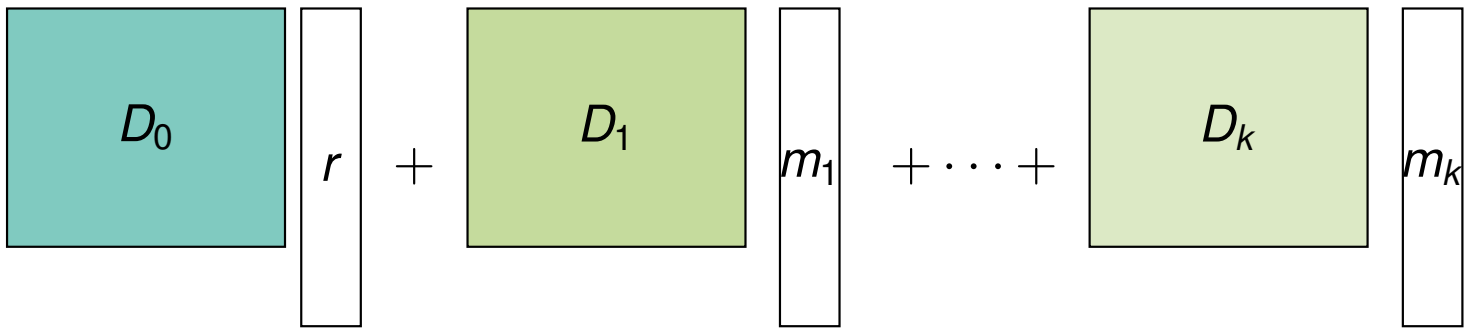
Operators can solve for $\mathsf{sk}_{\mathcal{U}}$.
Store these tags (with a serial number) in a database

Double-Spending Tags



SIS Commitments [KTX08]

Let $m = (m_1, \ldots, m_k) \in (\{0,1\}^m)^k, D_0, D_1, \ldots D_k \in \mathbb{Z}_q^{n \times m}, r \leftarrow \mathbb{Z}_q^m$

$\mathrm{Com}(m; r) :=$ 

SIS Commitments - Block Substitution

Block Substitution

Let $m_i \neq \tilde{m}_i$.

$$c := D_0 \cdot r + D_1 \cdot m_1 + \cdots + D_k \cdot m_k$$

$$\text{Subst}(c, m_i, \tilde{m}_i) := c - D_i \cdot m_i + D_i \cdot \tilde{m}_i$$

$\text{Subst}(c, m_i, \hat{m}_i)$ is a valid commitment on $\tilde{m}_i$

Lattice-based Construction

Example: *Accumulation*-Protocol to get points:

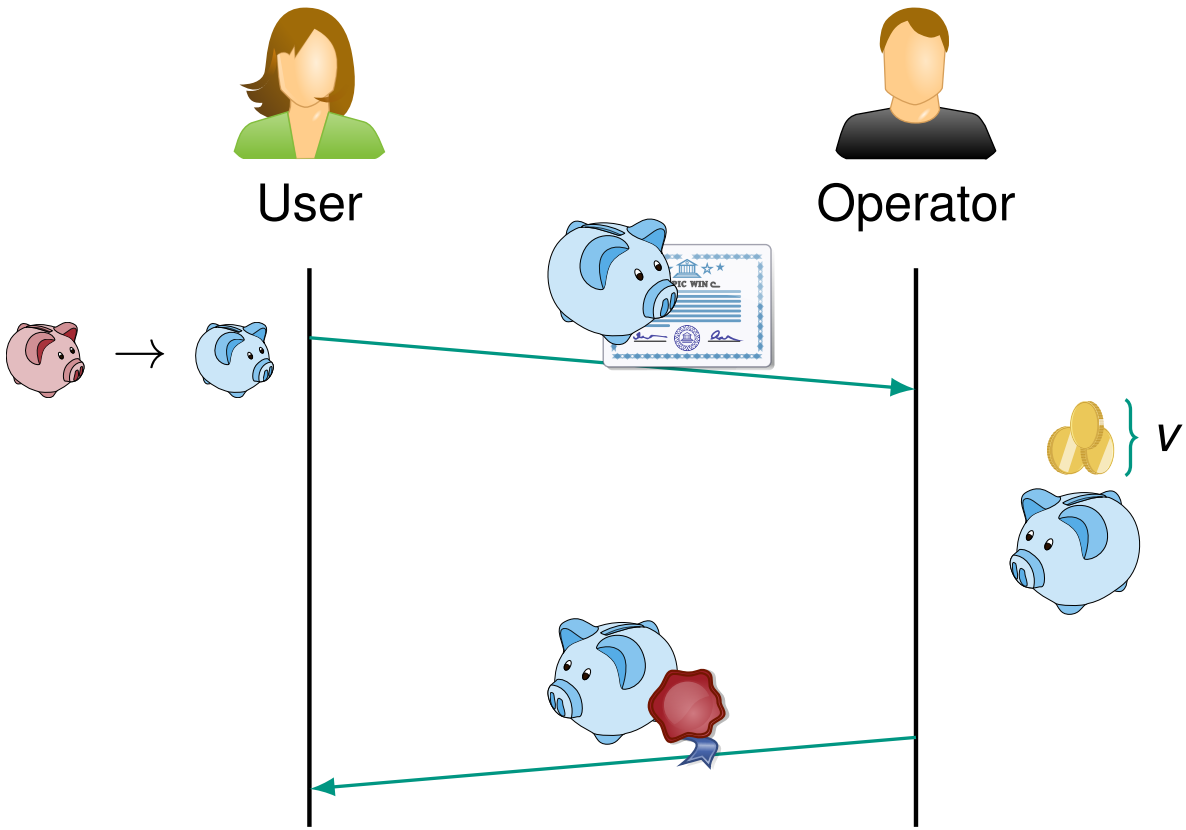


Figure: Accumulation-Protocol, graphics by M. Nagel

Lattice-based Construction

Example: *Accumulation*-Protocol to get points:

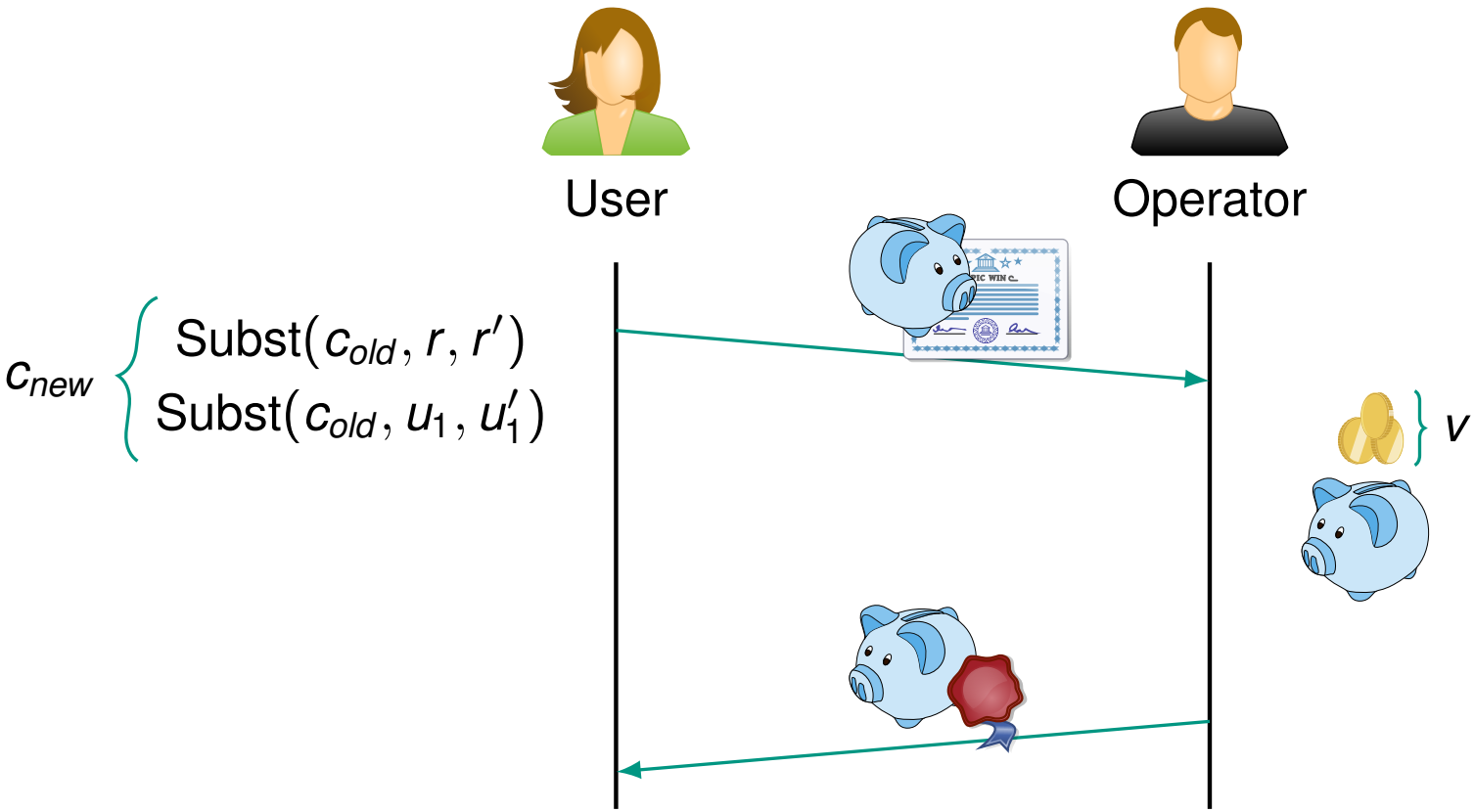


Figure: Accumulation-Protocol, graphics by M. Nagel

Lattice-based Construction

Example: *Accumulation*-Protocol to get points:

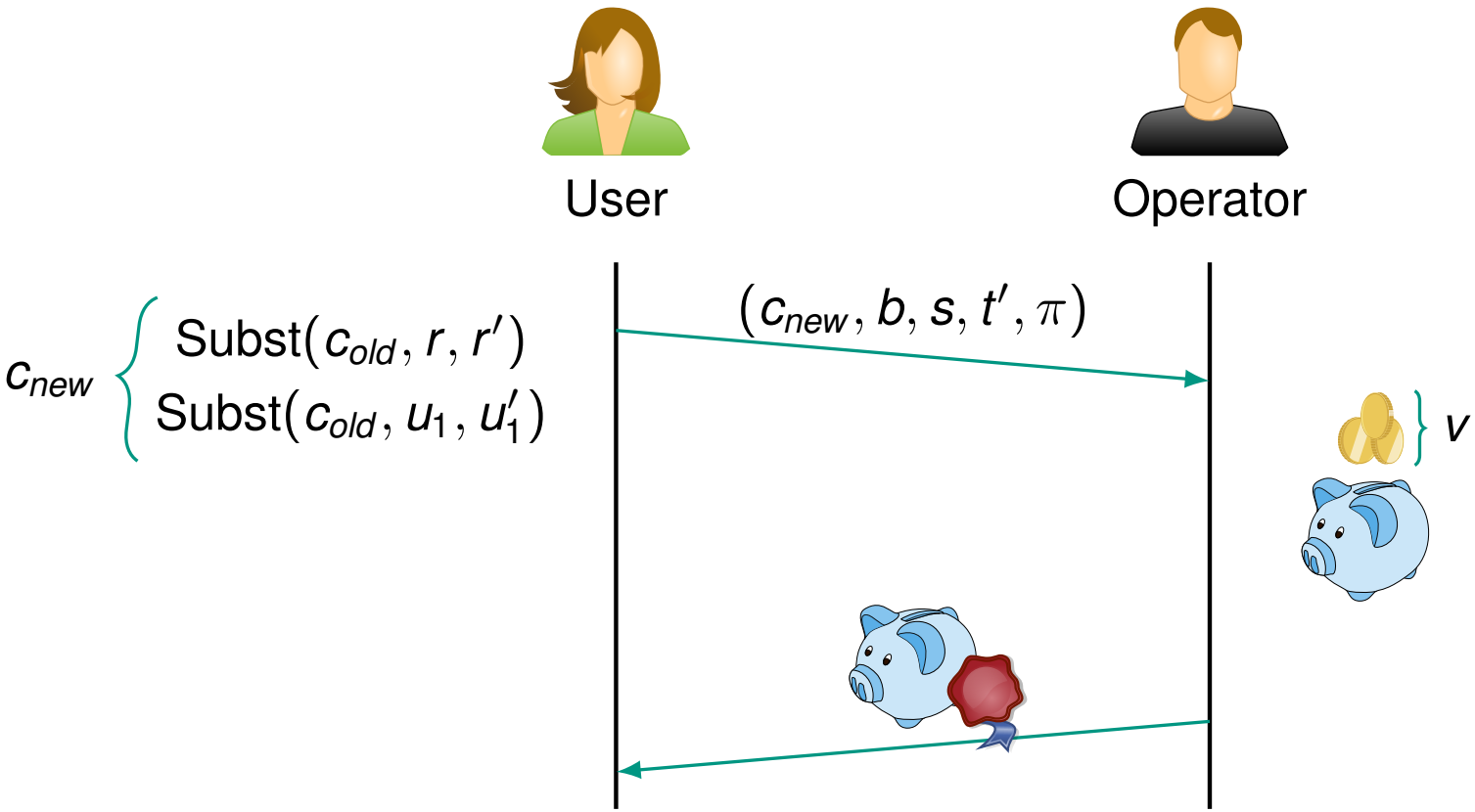


Figure: Accumulation-Protocol, graphics by M. Nagel

Lattice-based Construction

Example: *Accumulation*-Protocol to get points:

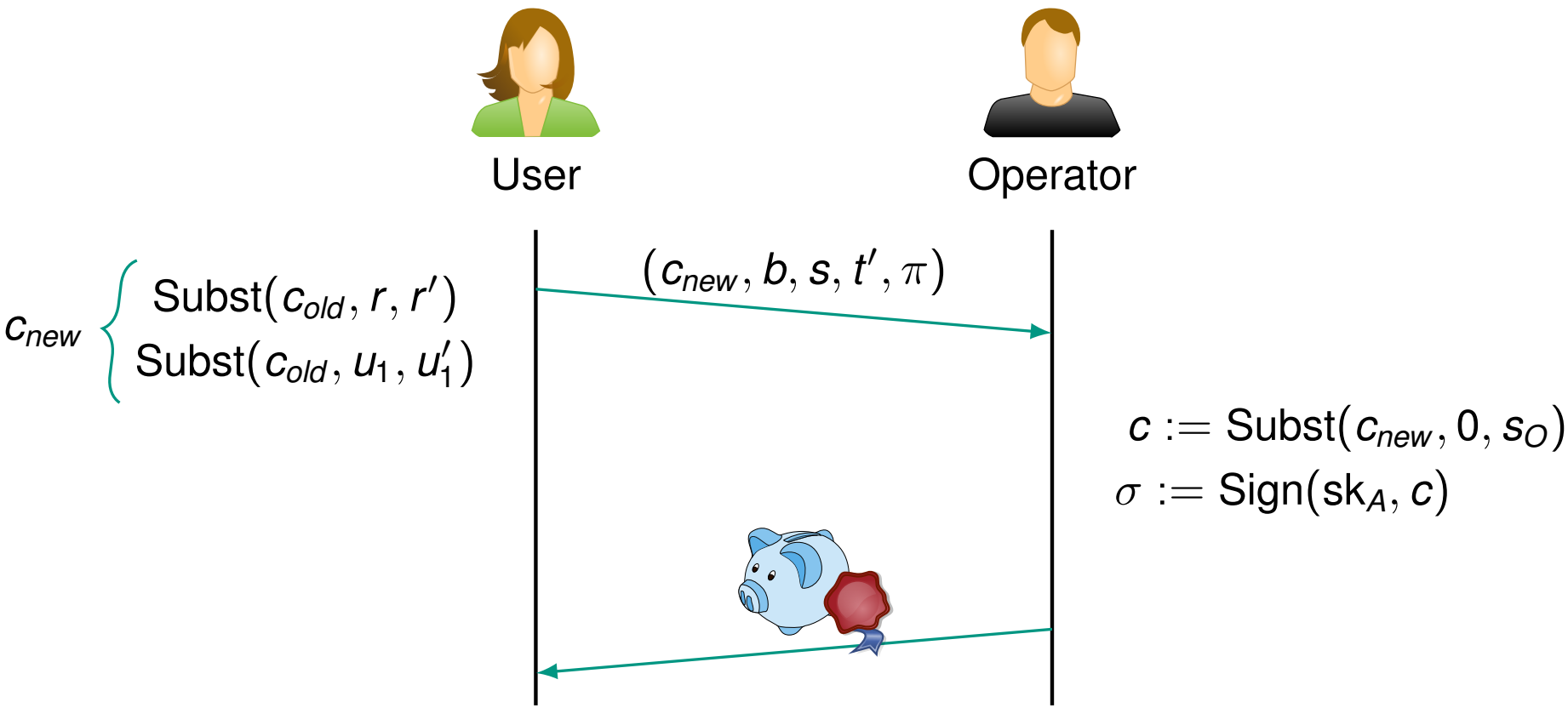


Figure: Accumulation-Protocol, graphics by M. Nagel

Lattice-based Construction

Example: *Accumulation*-Protocol to get points:

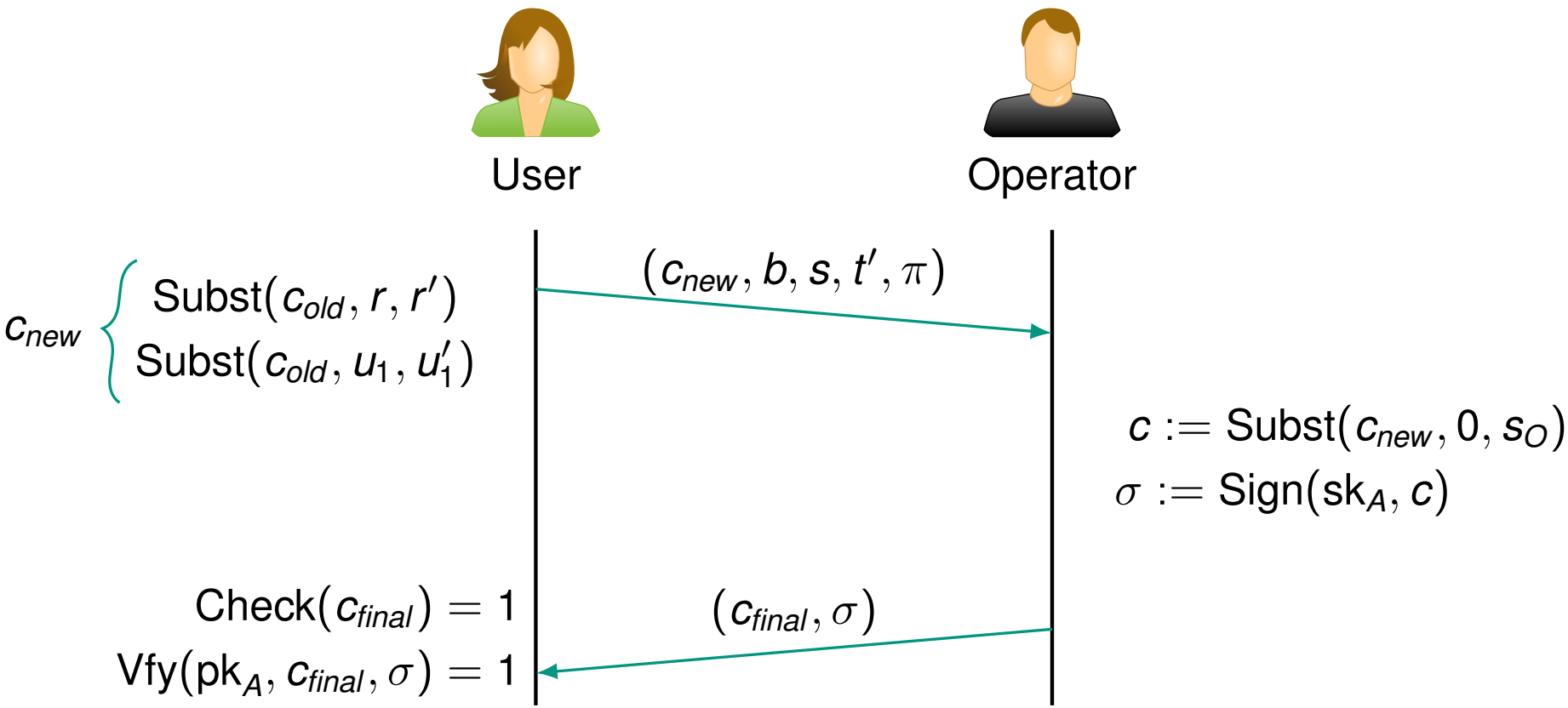
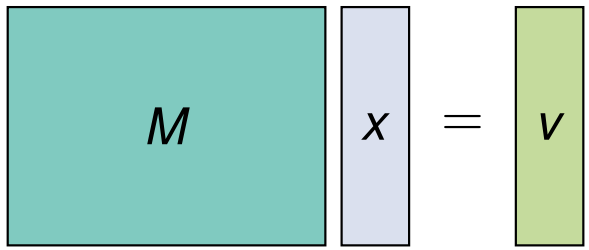


Figure: Accumulation-Protocol, graphics by M. Nagel

Zero-Knowledge Proof [Yan+19]

Statement of the form

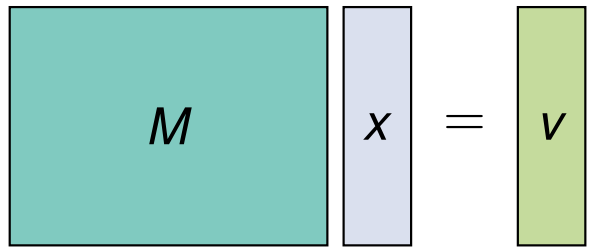


and additionally multiplicative relations:

$$\forall (h, i, j) \in \mathcal{M} : x[h] = x[i] \cdot x[j]$$

Zero-Knowledge Proof [Yan+19]

Statement of the form



and additionally multiplicative relations:

$$\forall (h, i, j) \in \mathcal{M} : x[h] = x[i] \cdot x[j]$$

E.g. ensure that vectors are binary: $\mathcal{M} = \{(i, i, i) \mid i \in \{1, \ldots, n\}\}$.

Zero-Knowledge Proof [Yan+19]

Zero-Knowledge Proofs ensures that:

- Valid signature on token
- Double-spending tag correct
- Commitment contains user's secret key and balance
- Balance is right
- Witness has small norm

Choice of parameters

Used the root Hermite factor estimation formulas of [Yan+19] for SIS/LWE instances

Goal:

RHF ≤ 1.0048. Corresponds to 80-bit security.

Choice of parameters

Used the root Hermite factor estimation formulas of [Yan+19] for SIS/LWE instances

Goal:

RHF ≤ 1.0048. Corresponds to 80-bit security.

Instances:

- SIS for binding commitment
- SIS for the public-private key pair
- SIS for the signature to be secure.
- SIS and LWE for the zero-knowledge protocol [Yan+19].

Efficiency estimation

Protocol	Issuance	Transaction	Token	Based on
Our work	70 MB	199 MB	11 MB	Lattices
E-Cash [Lib+17]	33 TB	720 TB	4 MB	Lattices
E-Cash [Yan+19]	53 MB	262 MB	4 MB	Lattices
BBA+ [JR16]	1 kB	14 kB	$<$1 kB	Elliptic Curves
BBW [Har+17]	1 kB	5 kB	$<$1 kB	Elliptic Curves

Efficiency estimation

Protocol	Issuance	Transaction	Token	Based on
Our work	70 MB	199 MB	11 MB	Lattices
E-Cash [Lib+17]	33 TB	720 TB	4 MB	Lattices
E-Cash [Yan+19]	53 MB	262 MB	4 MB	Lattices
BBA+ [JR16]	1 kB	14 kB	$<$1 kB	Elliptic Curves
BBW [Har+17]	1 kB	5 kB	$<$1 kB	Elliptic Curves

However: Efficiency of transaction in our construction without ZK 1.8 MB

Conclusion

Results

- ✓ Lattice-based BBA construction
  - Construction is feasible
  - Communication cost high
  - Costs are comparable to other constructions

Future Work

Enhance efficiency

- Use structured lattices
- Find more efficient building blocks (mainly ZK)

Conclusion

Results

- ✓ Lattice-based BBA construction
  - Construction is feasible
  - Communication cost high
  - Costs are comparable to other constructions

Future Work

Enhance efficiency

- Use structured lattices
- Find more efficient building blocks (mainly ZK)

Bibliography I

Johannes Bloemer et al. “Updatable Anonymous Credentials and Applications to Incentive Systems”. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’19. New York, NY, USA: Association for Computing Machinery, Nov. 6, 2019, pp. 1671–1685. ISBN: 978-1-4503-6747-9. DOI: 10.1145/3319535.3354223.

Jan Bobolz et al. “Privacy-Preserving Incentive Systems with Highly Efficient Point-Collection”. In: *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*. ASIA CCS ’20. New York, NY, USA: Association for Computing Machinery, Oct. 5, 2020, pp. 319–333. ISBN: 978-1-4503-6750-9. DOI: 10.1145/3320269.3384769.

Bibliography II

Gunnar Hartung et al. “BBA+: Improving the Security and Applicability of Privacy-Preserving Point Collection”. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’17. New York, NY, USA: Association for Computing Machinery, Oct. 30, 2017, pp. 1925–1942. ISBN: 978-1-4503-4946-8. DOI: 10.1145/3133956.3134071.

Max Hoffmann et al. “Black-Box Wallets: Fast Anonymous Two-Way Payments for Constrained Devices”. In: *Proceedings on Privacy Enhancing Technologies* 2020.1 (2020), pp. 165–194. DOI: 10.2478/popets-2020-0010.

Tibor Jager and Andy Rupp. “Black-Box Accumulation: Collecting Incentives in a Privacy-Preserving Way”. In: *Proceedings on Privacy Enhancing Technologies* 2016.3 (2016), pp. 62–82. DOI: 10.1515/popets-2016-0016.

Bibliography III

Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa. “Concurrently Secure Identification Schemes Based on the Worst-Case Hardness of Lattice Problems”. In: *Advances in Cryptology - ASIACRYPT 2008*. Ed. by Josef Pieprzyk. Vol. 5350. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 372–389. ISBN: 978-3-540-89254-0 978-3-540-89255-7. DOI: 10.1007/978-3-540-89255-7_23.

Benoît Libert et al. “Zero-Knowledge Arguments for Lattice-Based PRFs and Applications to E-Cash”. In: *Advances in Cryptology – ASIACRYPT 2017*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10626. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017, pp. 304–335. ISBN: 978-3-319-70699-3 978-3-319-70700-6. DOI: 10.1007/978-3-319-70700-6_11.

Bibliography IV

Rupeng Yang et al. “Efficient Lattice-Based Zero-Knowledge Arguments with Standard Soundness: Construction and Applications”. In: *Advances in Cryptology – CRYPTO 2019*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11692. Cham: Springer International Publishing, 2019, pp. 147–175. ISBN: 978-3-030-26947-0 978-3-030-26948-7. DOI: 10.1007/978-3-030-26948-7_6.