A Compact Signature Scheme Based on Ideal Lattices

Keita Xagawa/Keisuke Tanaka (Tokyo Tech)

Results

Gentry, Peikert, Vaikuntanathan (2008)	Ours
Signature Scheme	Signature Scheme
Based on Lattices	… on Ideal Lattices
Large vk	Small vk

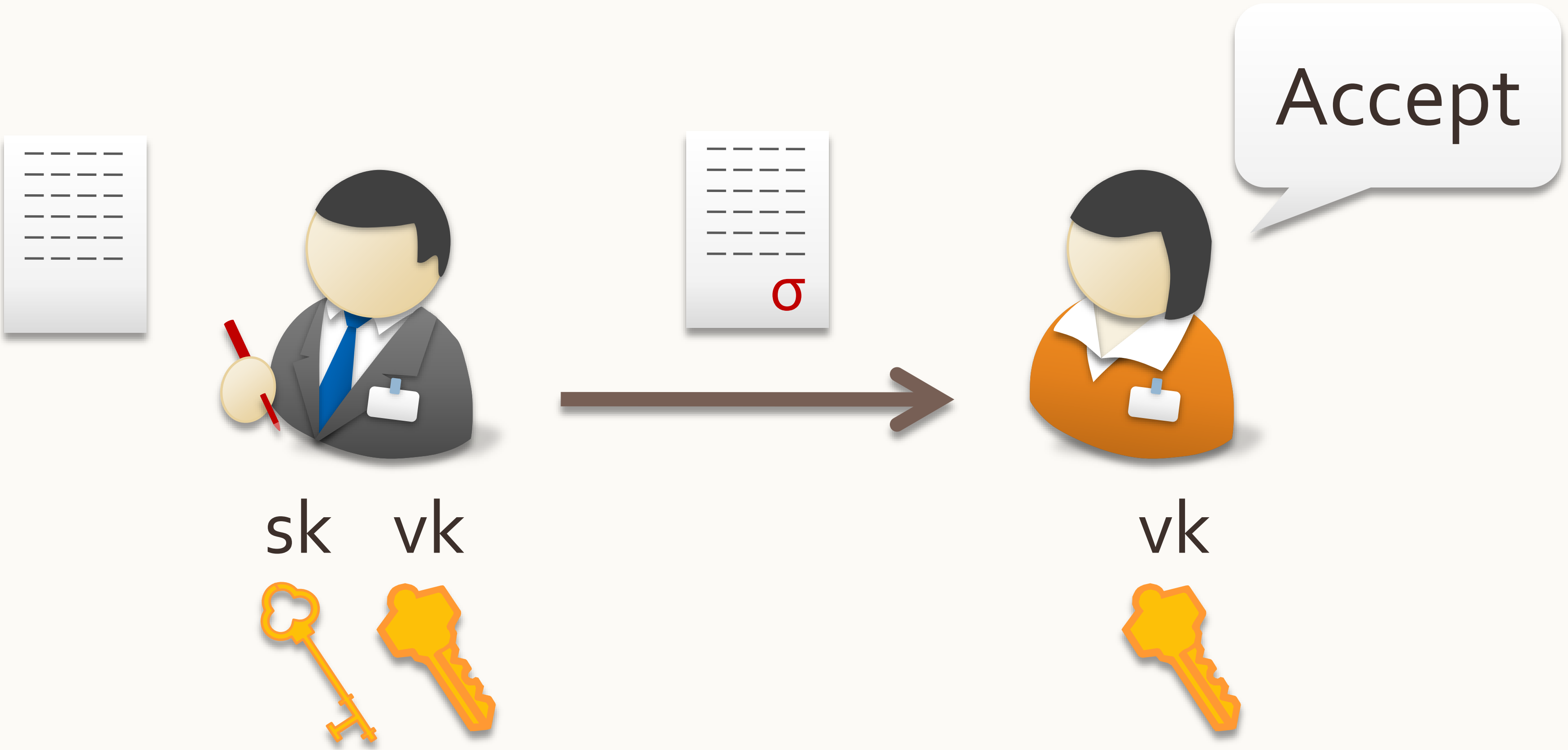
Agenda

- Signature schemes
- Lattice problems
- The GPV signature scheme
  - Lattice-based hash functions
  - Ajtai's algorithm
- Our scheme
  - Ideal-lattice-based hash functions
  - Our algorithm
- Comparison GPV and ours

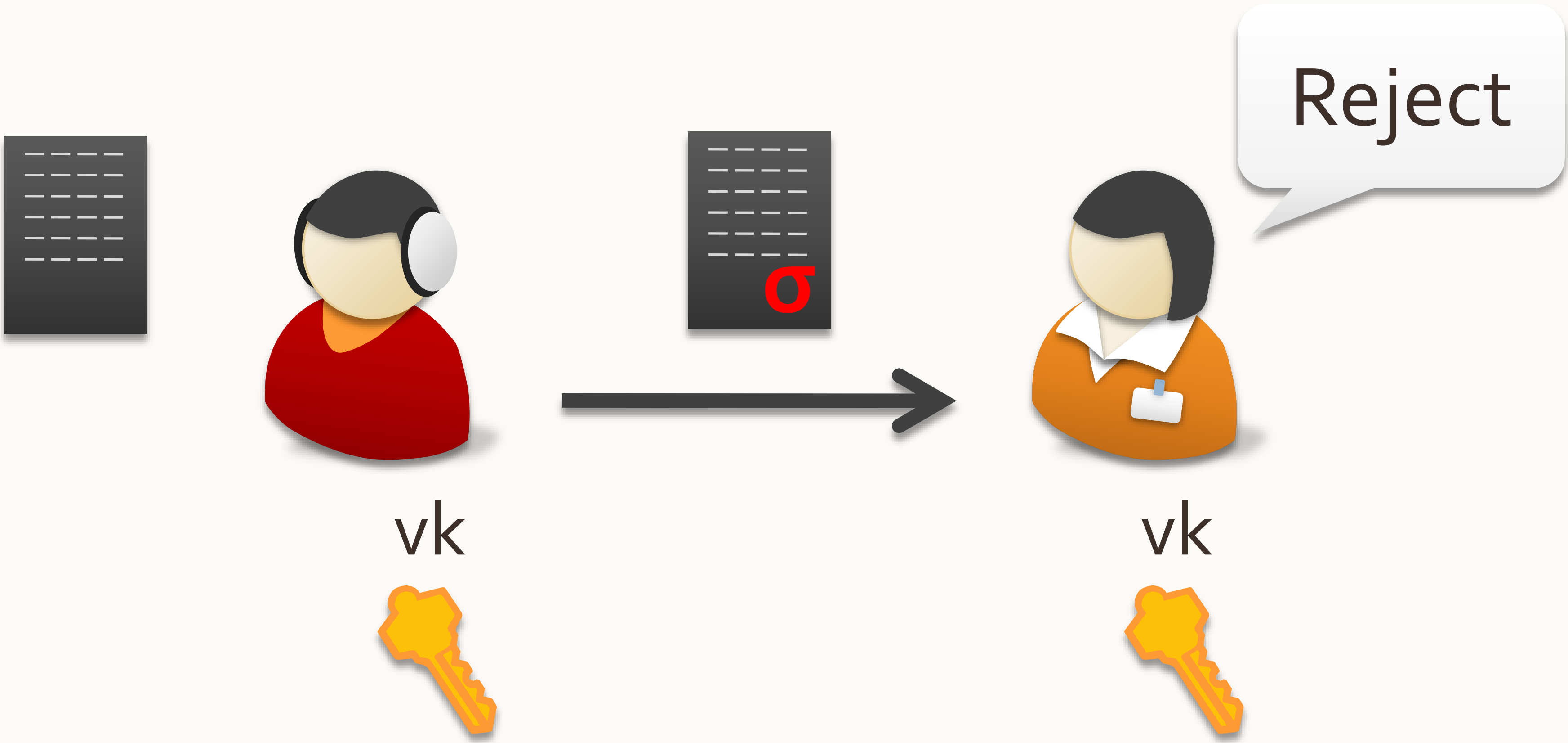
Agenda

- Signature schemes
- Lattice problems
- The GPV signature scheme
  - Lattice-based hash functions
  - Ajtai's algorithm
- Our scheme
  - Ideal-lattice-based hash functions
  - Our algorithm
- Comparison GPV and ours

Signature scheme

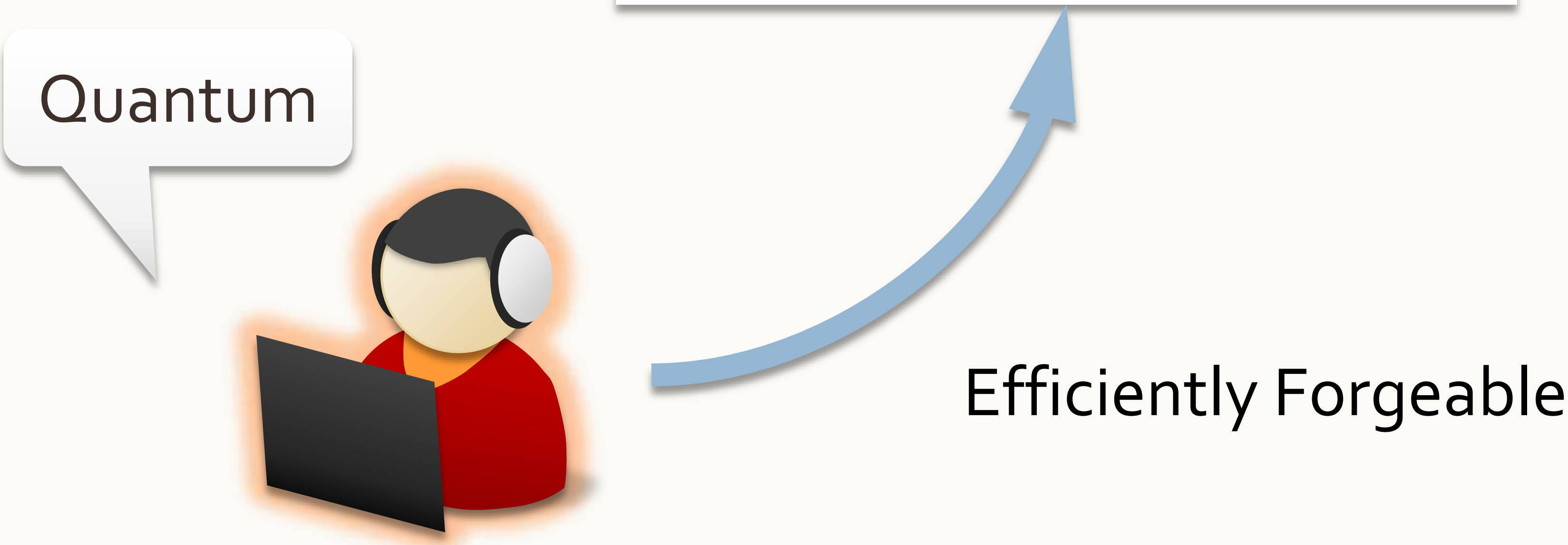


Signature scheme



A threat to digital signatures

- RSA Signature
- ElGamal Signature
- …

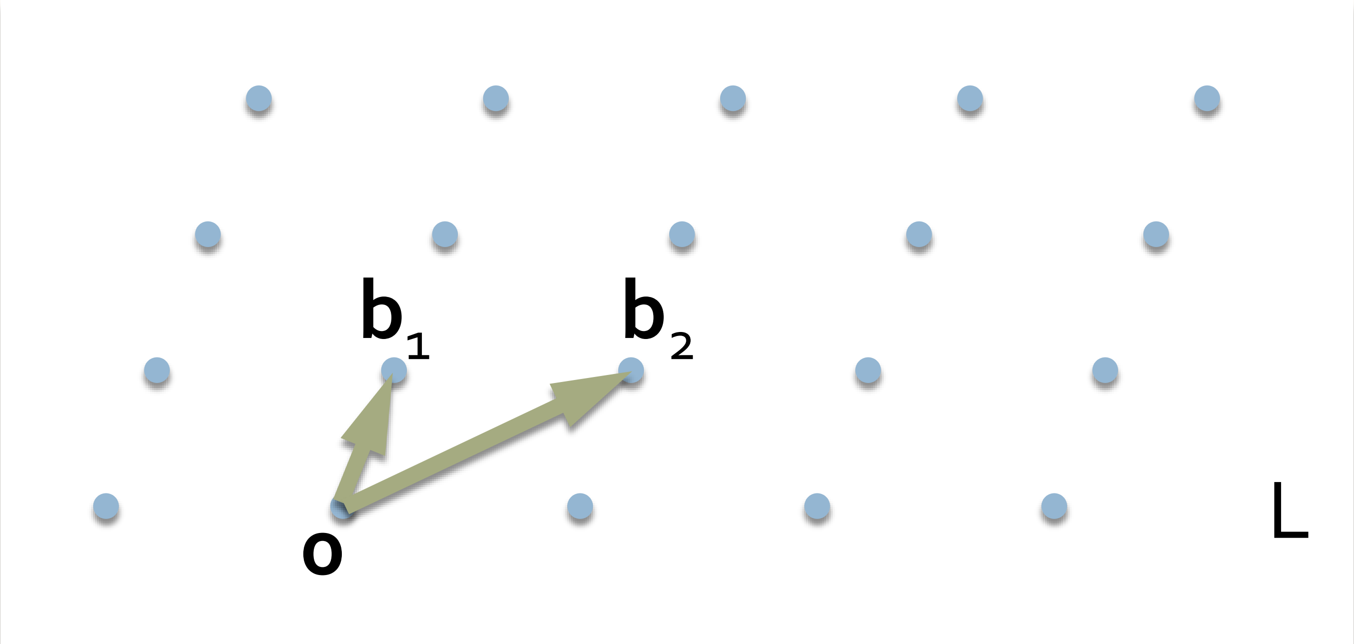


Agenda

- Signature schemes
- Lattice problems
- The GPV signature scheme
  - Lattice-based hash functions
  - Ajtai's algorithm
- Our scheme
  - Ideal-lattice-based hash functions
  - Our algorithm
- Comparison GPV and ours

Lattices

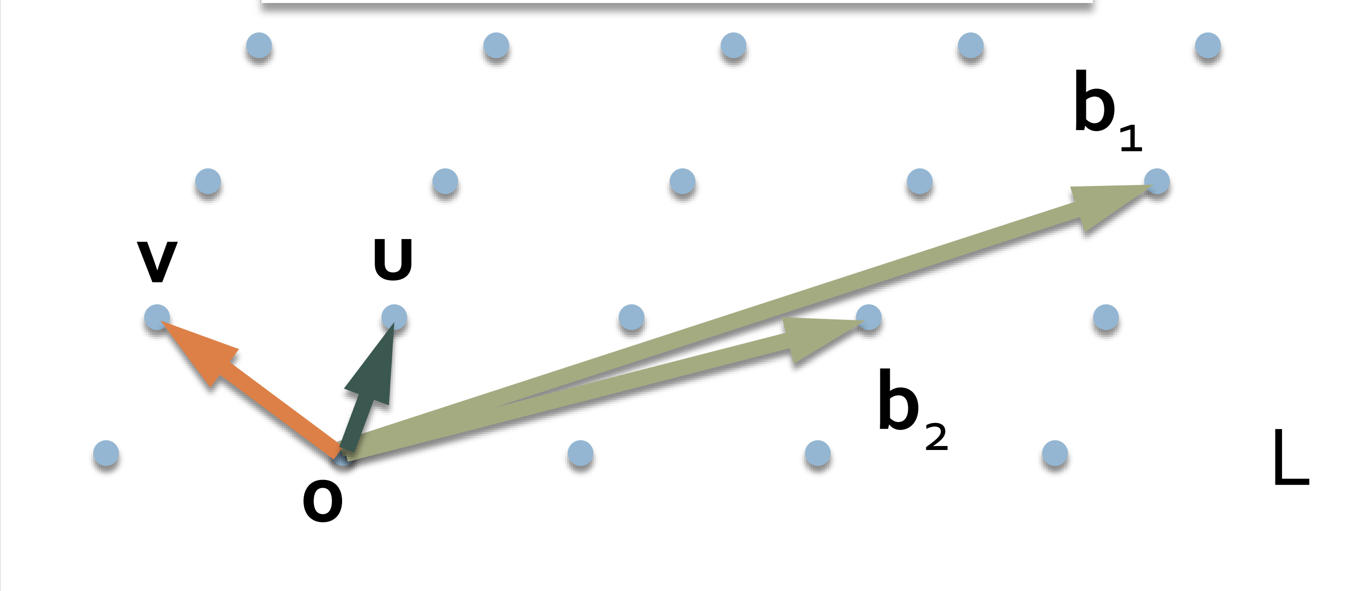
$$L=\{\sum_i \alpha_i \mathbf{b}_i : \alpha_i \in Z\}$$



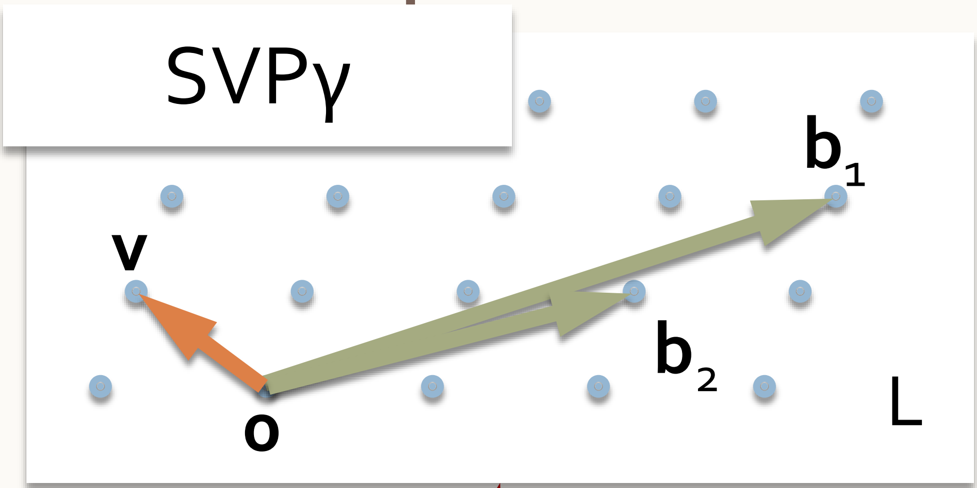
Shortest Vector Problem (SVPγ)

Input: L

Output: **v**



Importance of lattice problems



(Seems) hard

Agenda

- Signature schemes
- Lattice problems
- The GPV signature scheme
  - Lattice-based hash functions
  - Ajtai's algorithm
- Our scheme
  - Ideal-lattice-based hash functions
  - Our algorithm
- Comparison GPV and ours

The GPV signature scheme [GPV08]

Gentry

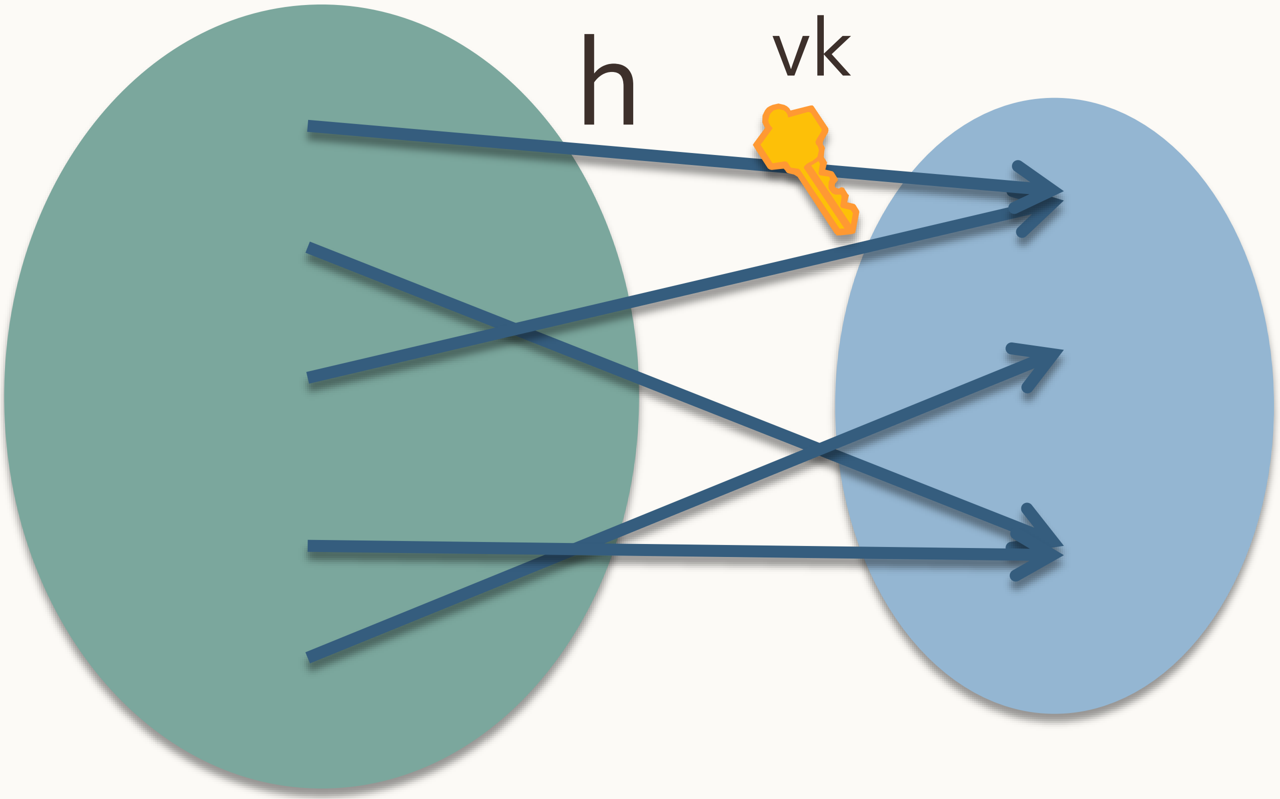
Peikert

vaikuntanathan

- Sig. scheme based on lattice

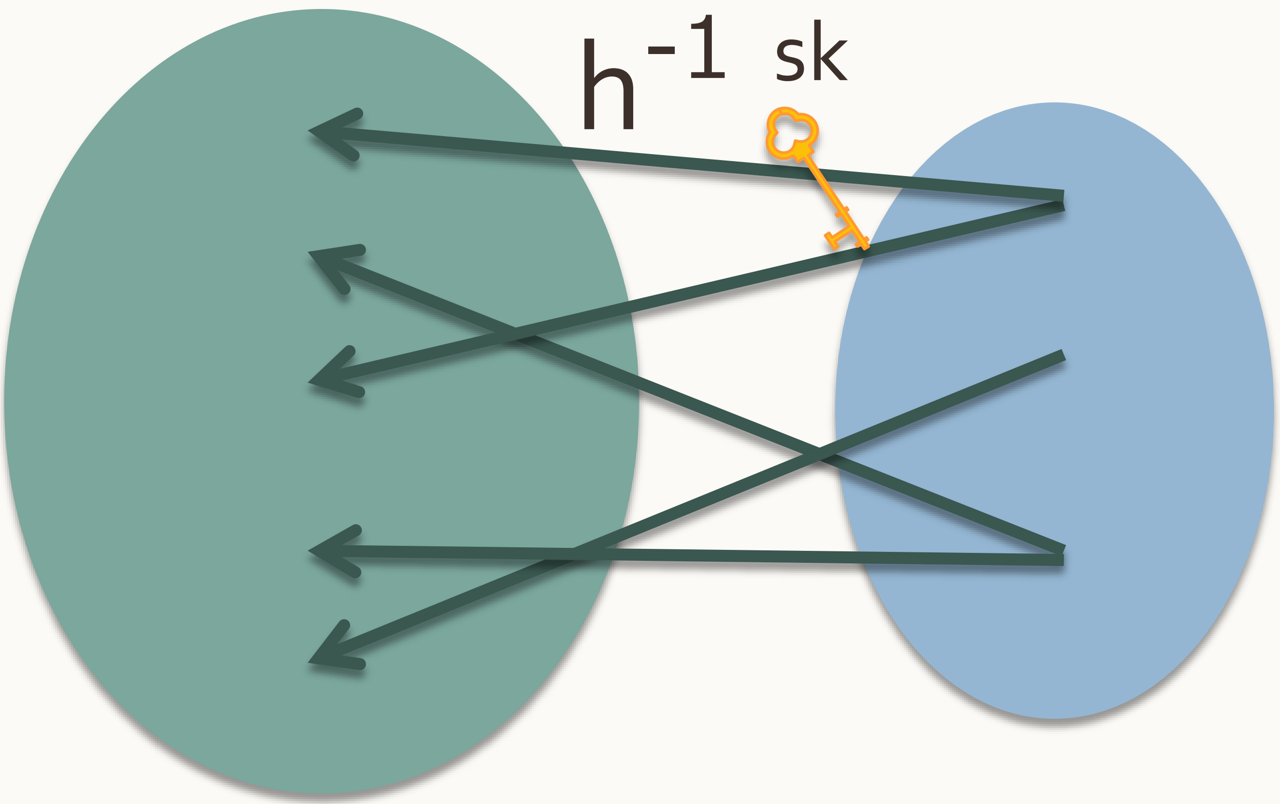
GPV sig. →

- CRHFs with trapdoors



GPV sig.←

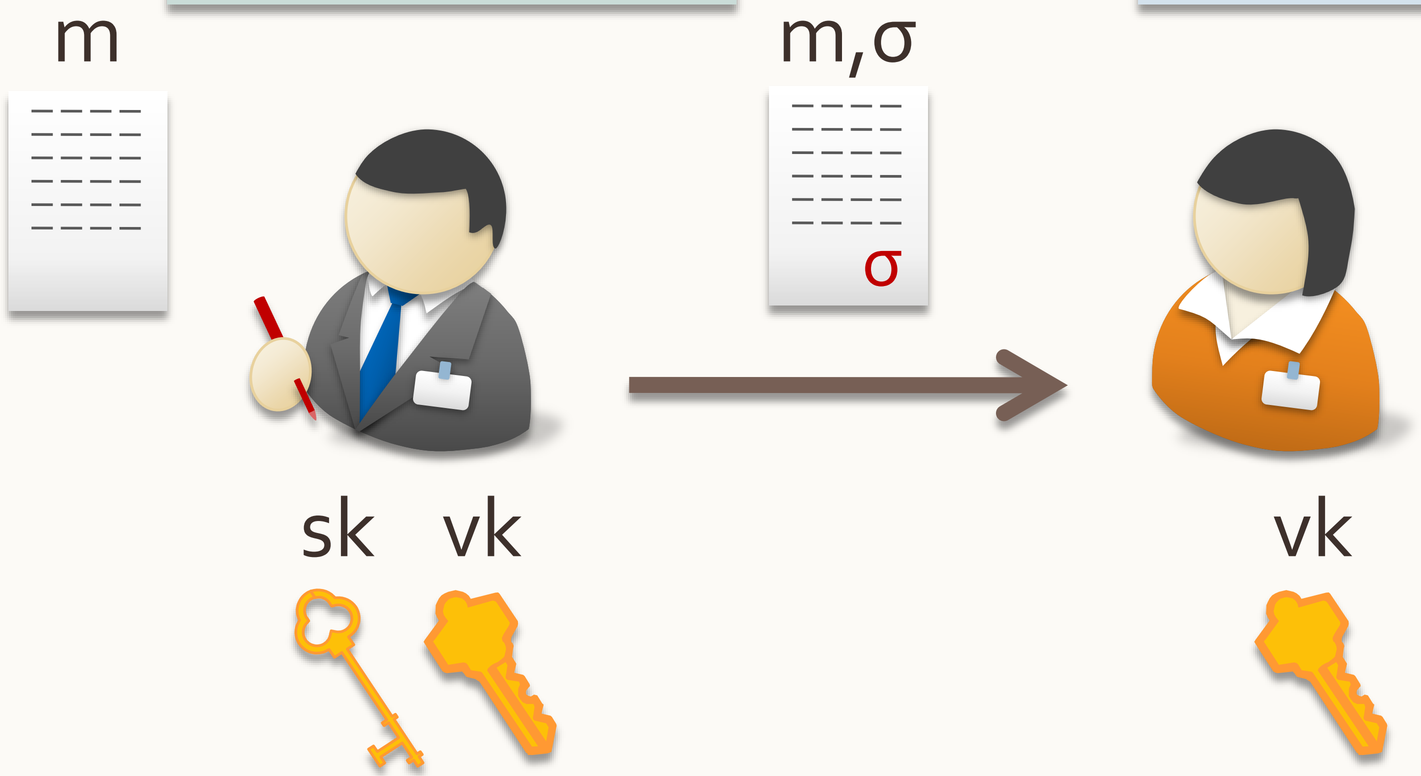
- CRHFs with trapdoors



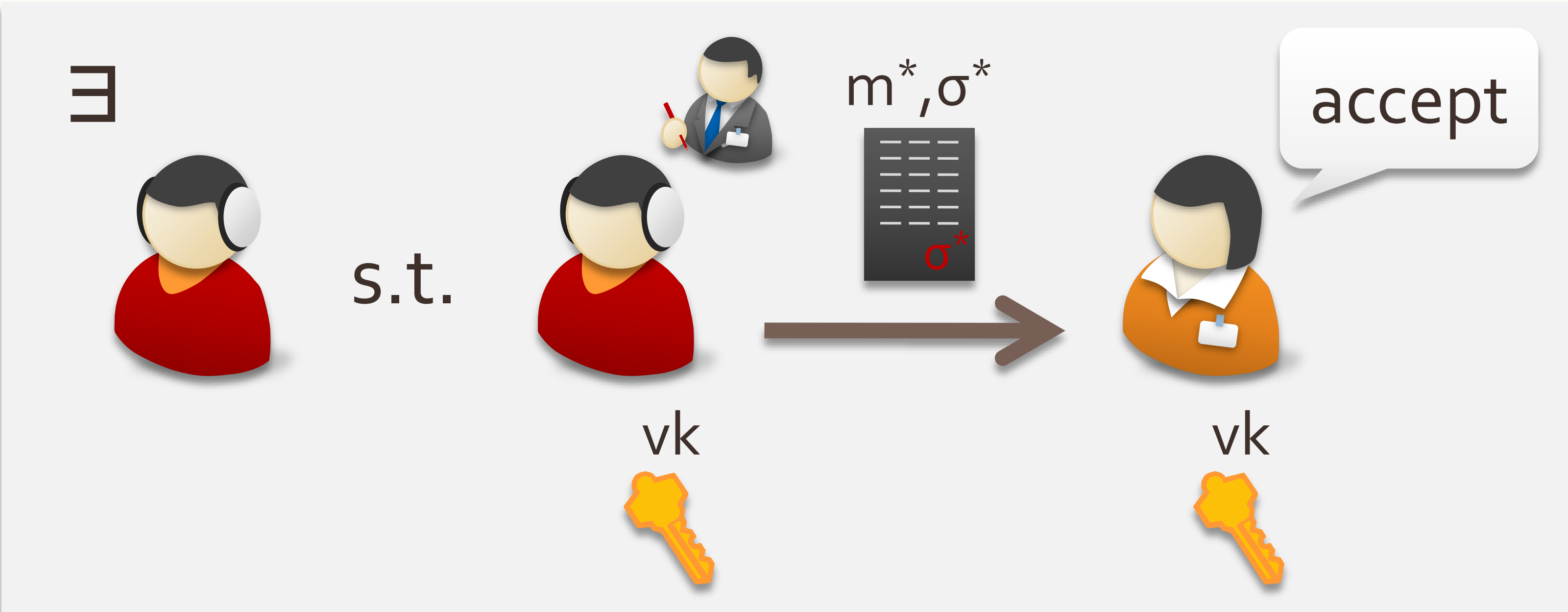
GPV sig. – Overview

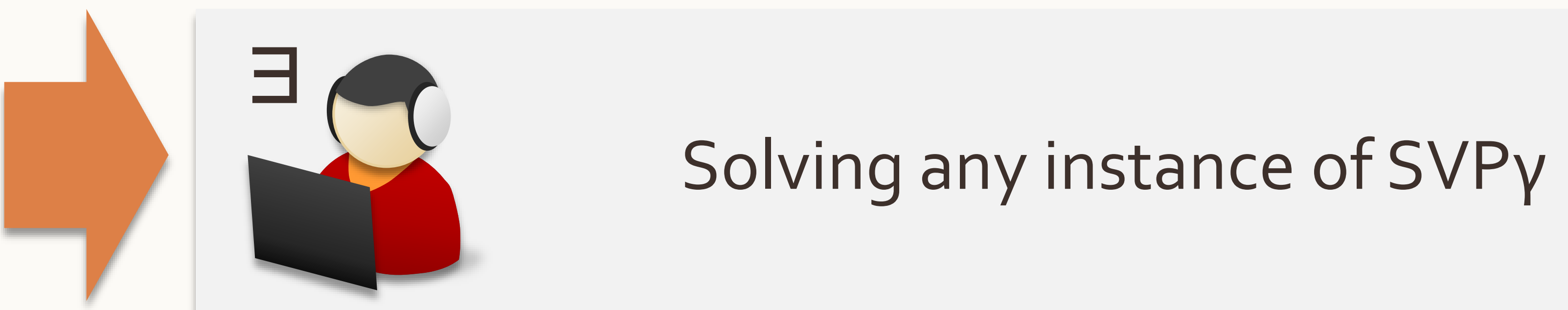
1. $H(m)$
2. $\sigma \leftarrow h^{-1}(H(m))$

1. $h(\sigma)=H(m)$?



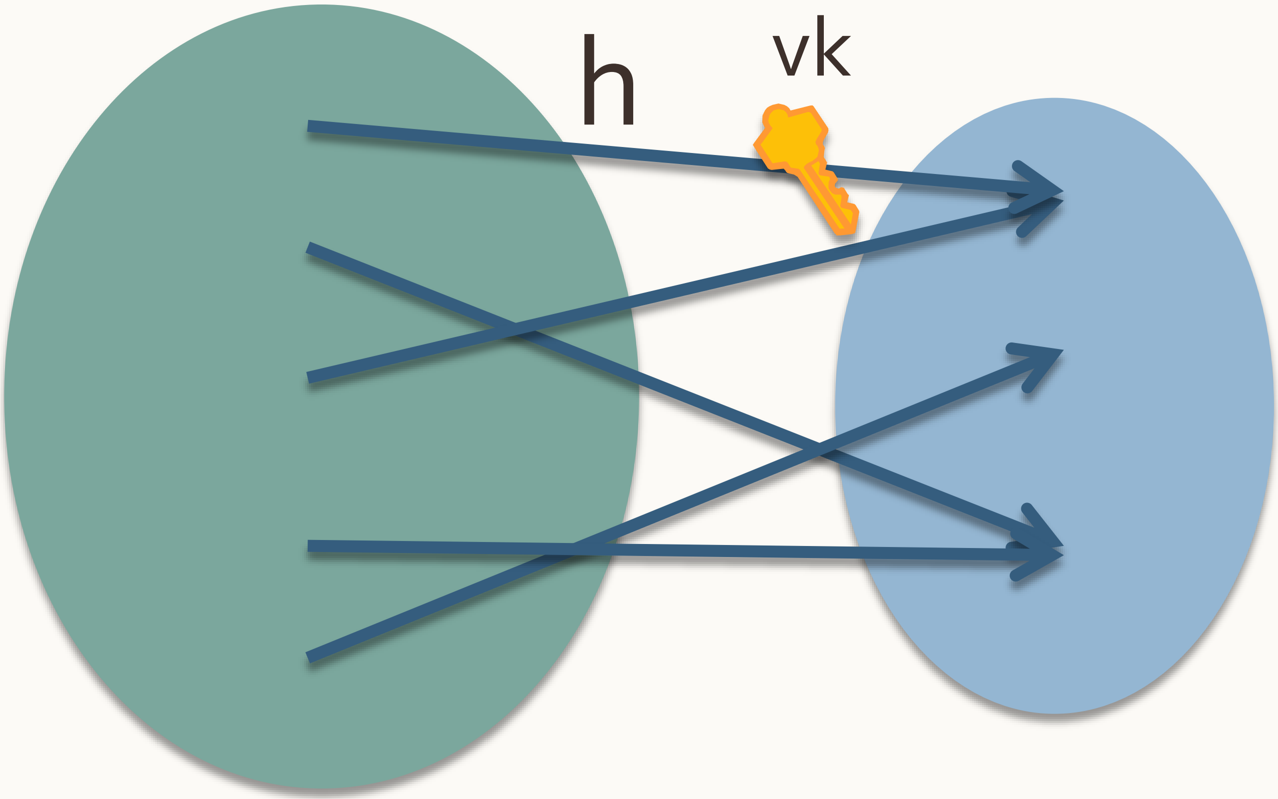
GPV sig. – Security





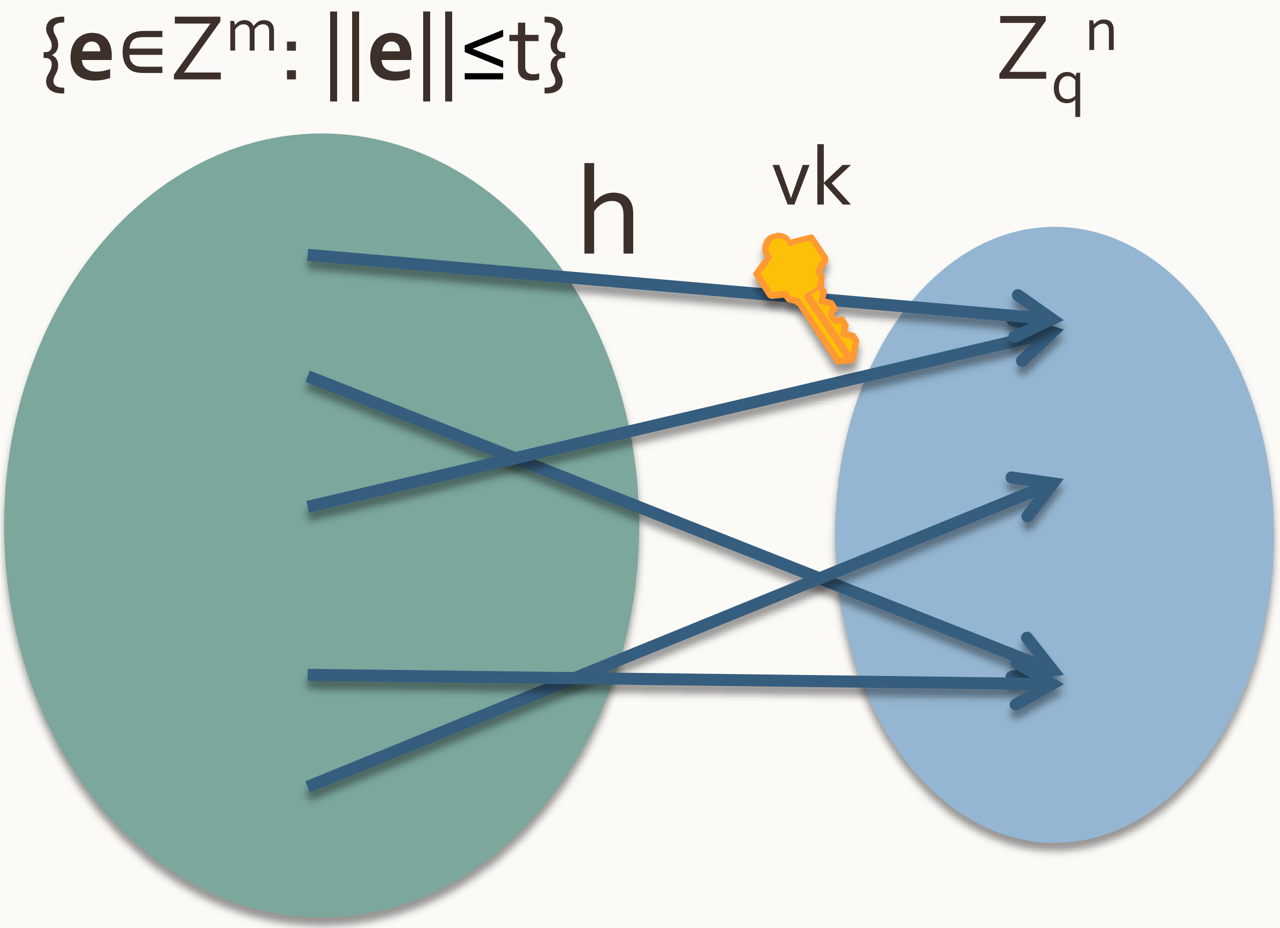
GPV Sig. →

- CRHFs with trapdoors



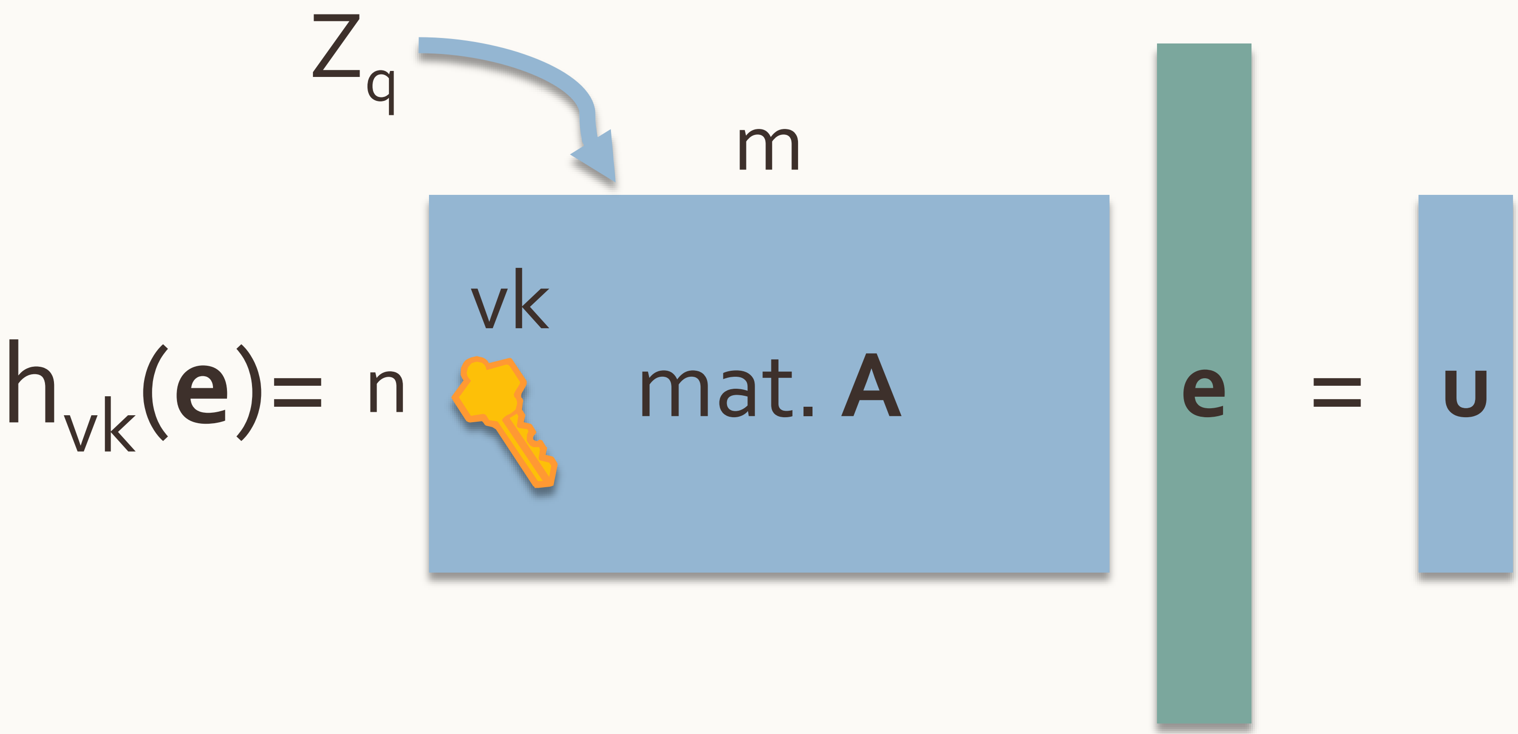
Lattice-based CRHFs [A96, …]

Ajtai



Lattice-based CRHFs [A96, …]

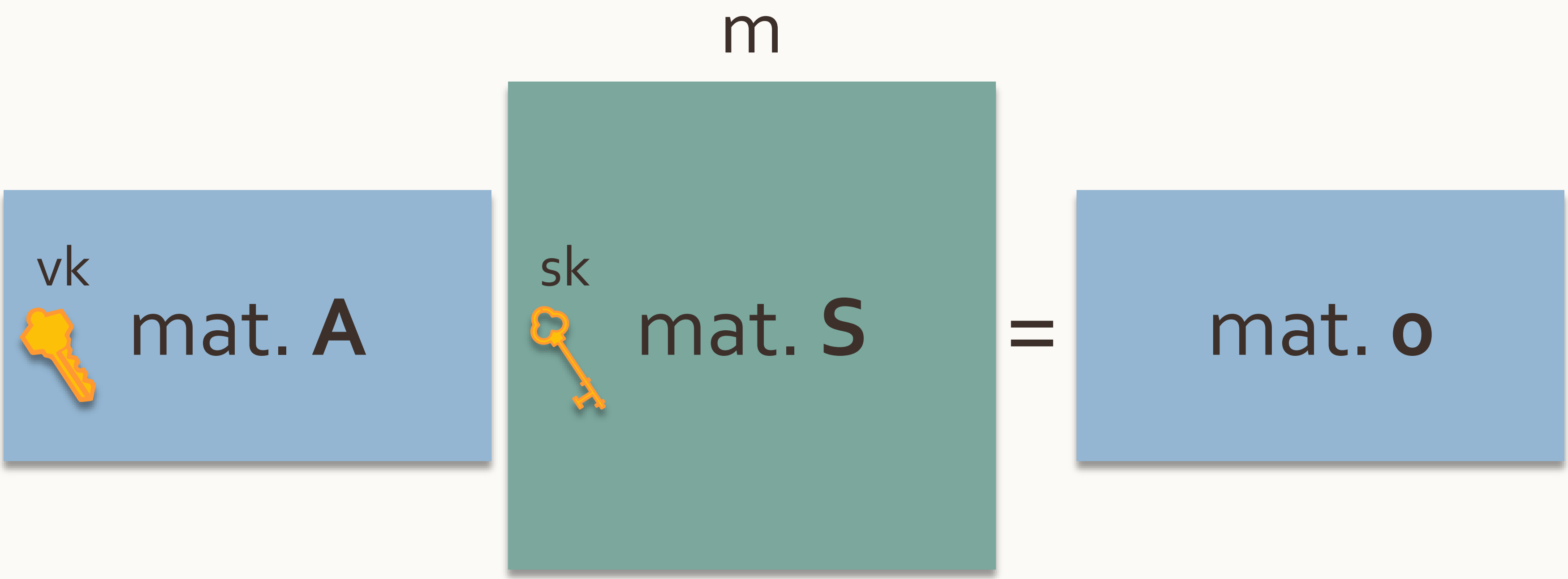
- $h_{vk}:\{\mathbf{e}\in Z^m : ||\mathbf{e}||\leq t\}\rightarrow Z_q^{\,n}$



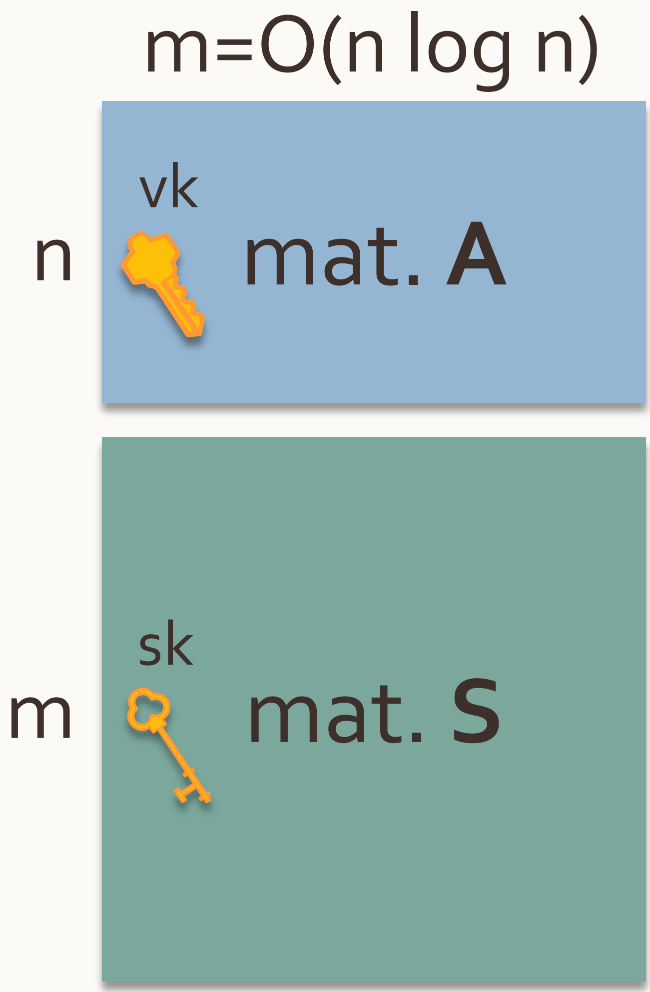
Trapdoor [A99, GPV08]

Ajtai

- Compose **A** and **S**



Problem in GPV sig.



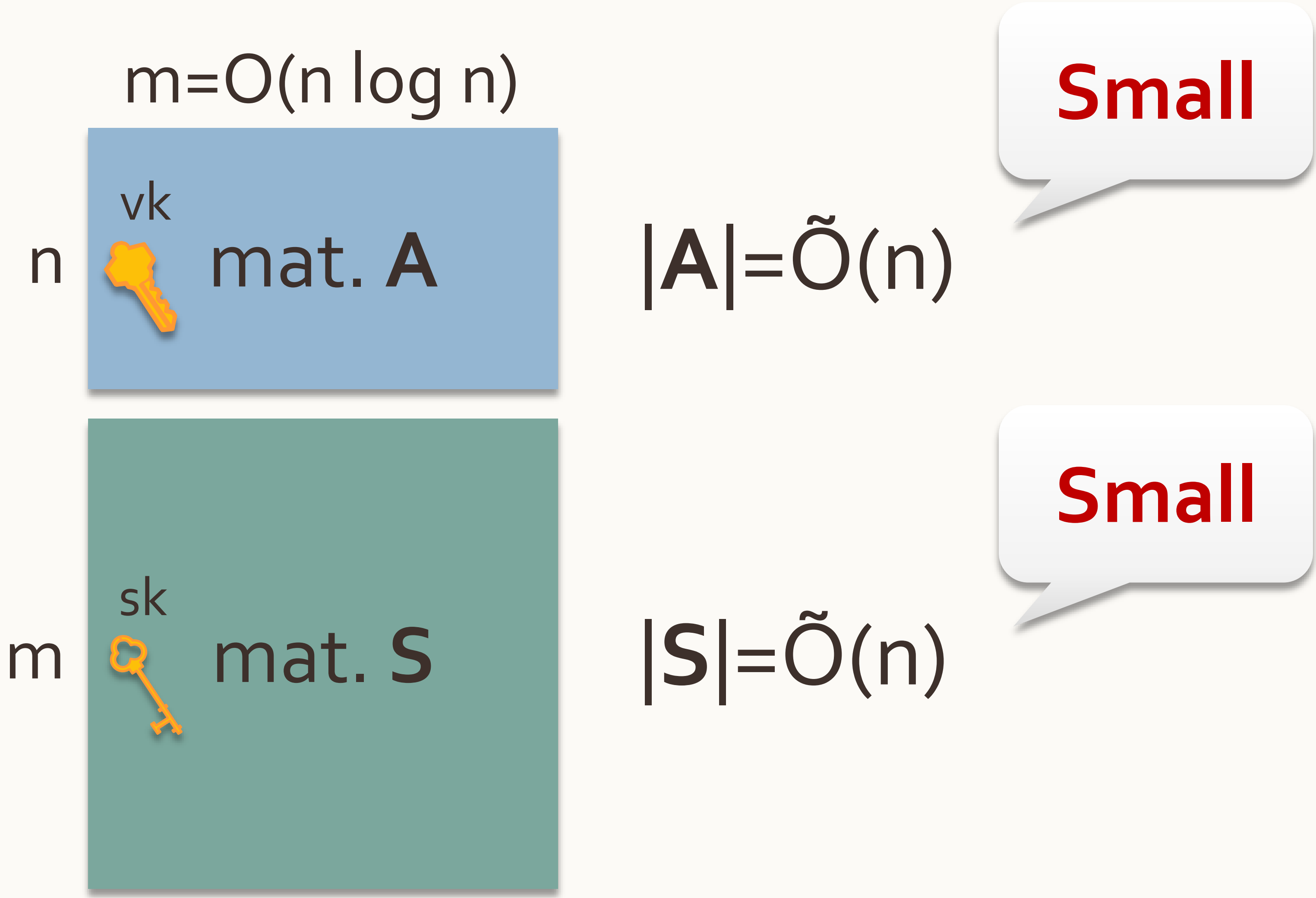
$|\mathbf{A}| = \tilde{O}(n^2)$

Huge!!

$|\mathbf{S}| = \tilde{O}(n^2)$

Huge!!

Our goal



Agenda

- Signature schemes
- Lattice problems
- The GPV signature scheme
  - Lattice-based hash functions
  - Ajtai's algorithm
- Our scheme
  - Ideal-lattice-based hash functions
  - Our algorithm
- Comparison GPV and ours

Main Idea

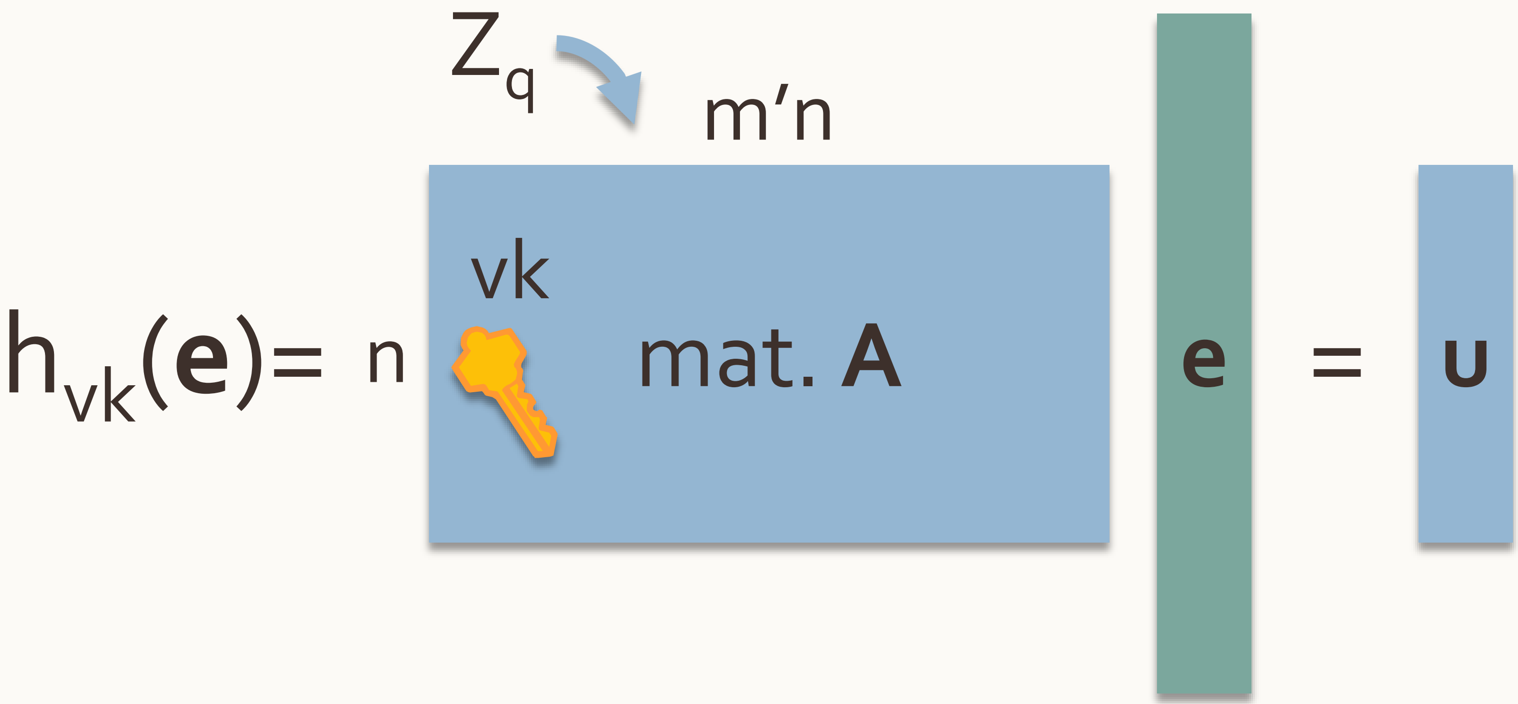
Gentry, Peikert, Vaikuntanathan (2008)	Ours
▫ Hash functions **Lattice-based** ▫ Trapdoor **Ajtai's algorithm**	▫ Hash functions **Ideal-lattice-based** ▫ Trapdoor **Our algorithm**

Ideal-lattice-based CRHFs [LM06]

Lyubashevsky

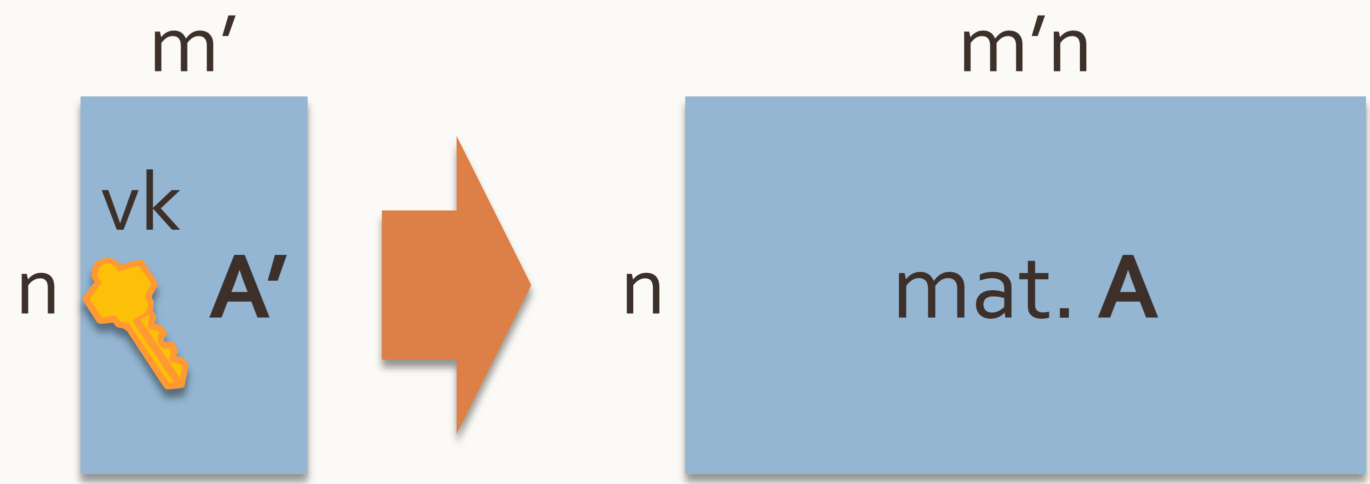
Micciancio

- $h_{vk}: \{\mathbf{e} \in Z^{m'n} : \|\mathbf{e}\| \le t\} \rightarrow Z_q^{\,n}$



Ideal-lattice-based CRHFs [LM06]

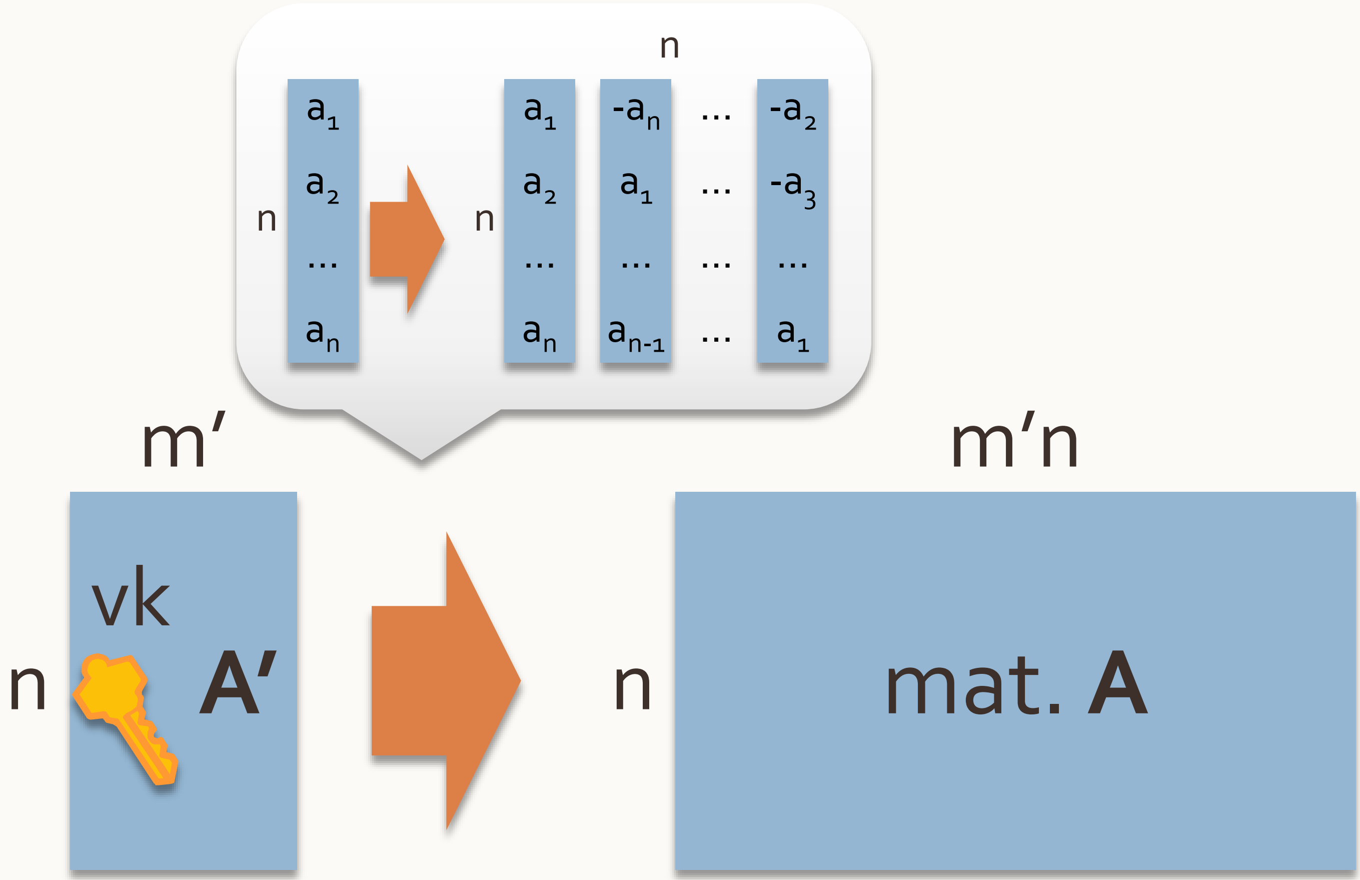
m'=O(log n)



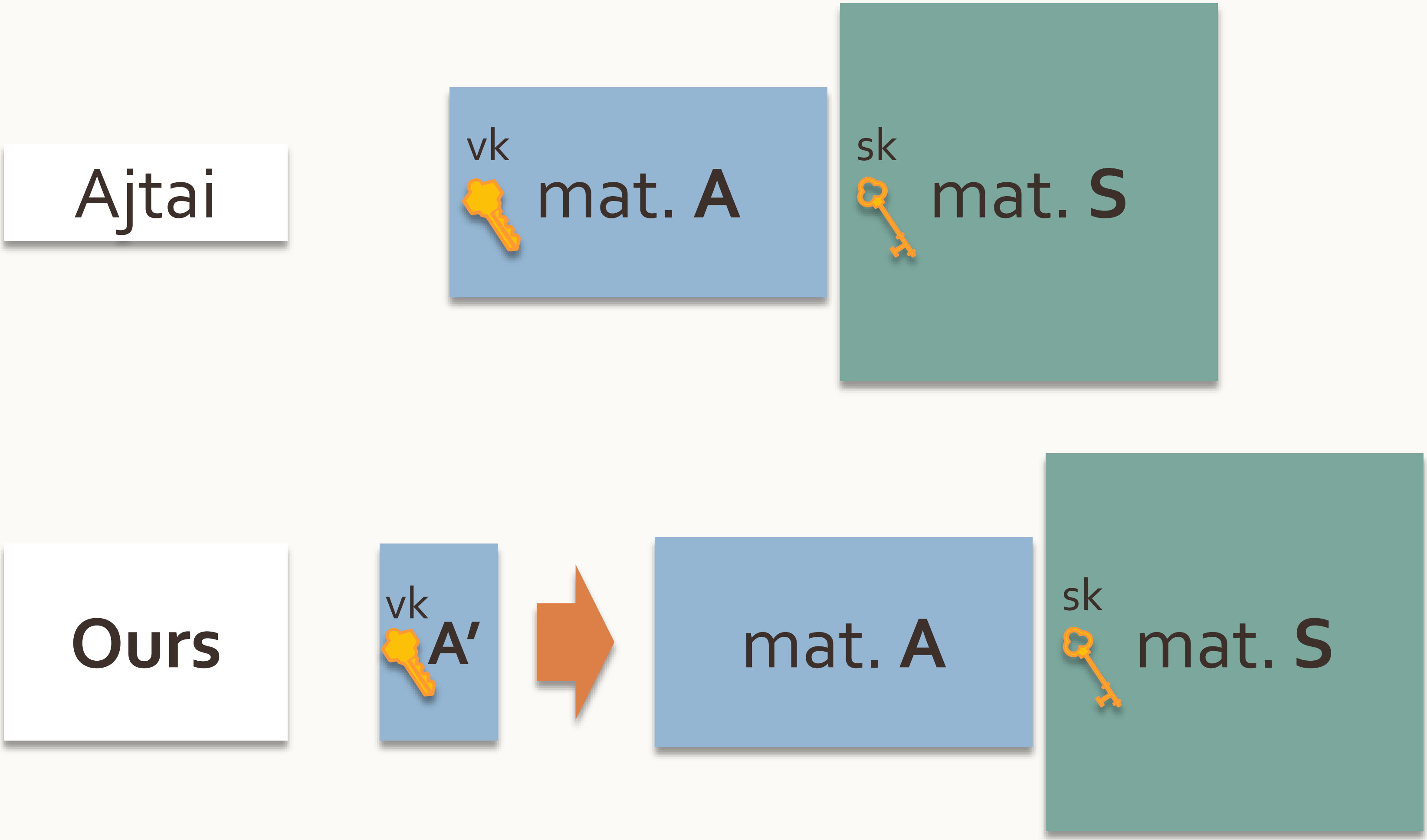
Ideal-lattice-based CRHFs [LM06]

$$
n \begin{bmatrix} a_1 \\ a_2 \\ \cdots \\ a_n \end{bmatrix}
\Rightarrow
\begin{array}{c} \\ n \end{array}
\begin{array}{c} n \\ \begin{bmatrix} a_1 & -a_n & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \cdots & \cdots & \cdots & \cdots \\ a_n & a_{n-1} & \cdots & a_1 \end{bmatrix} \end{array}
$$

Ideal-lattice-based CRHFs [LM06]

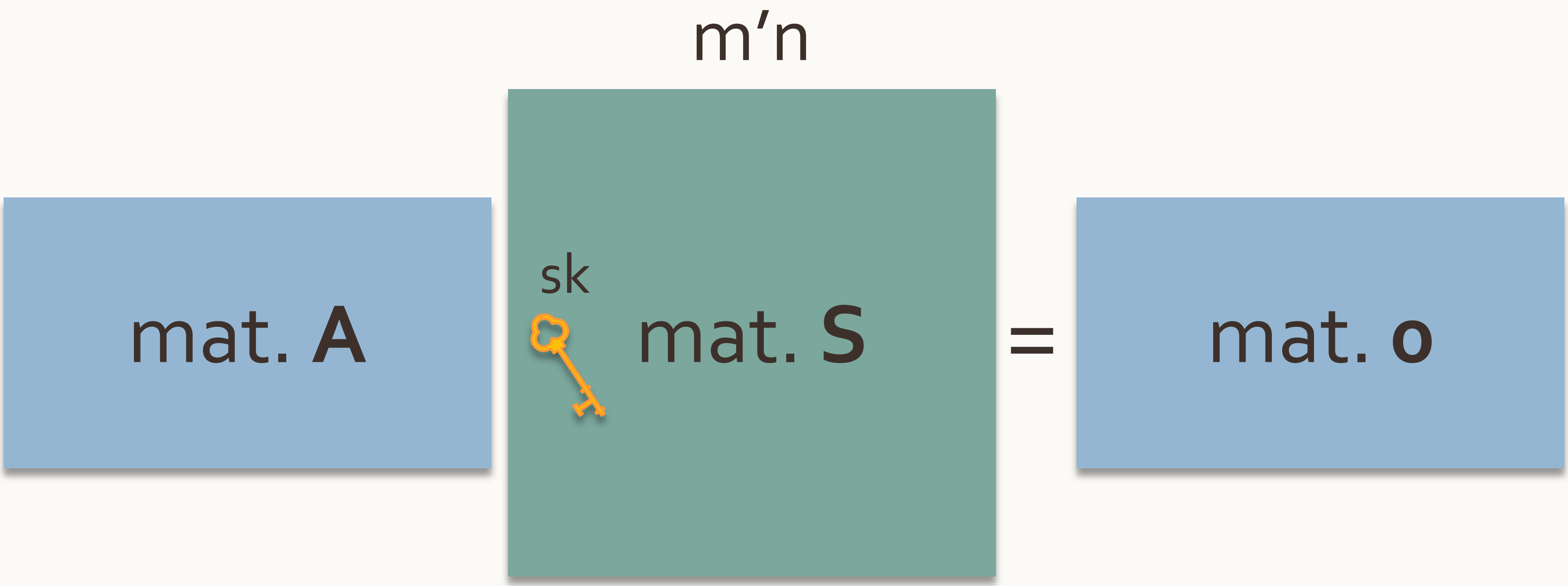


Trapdoors

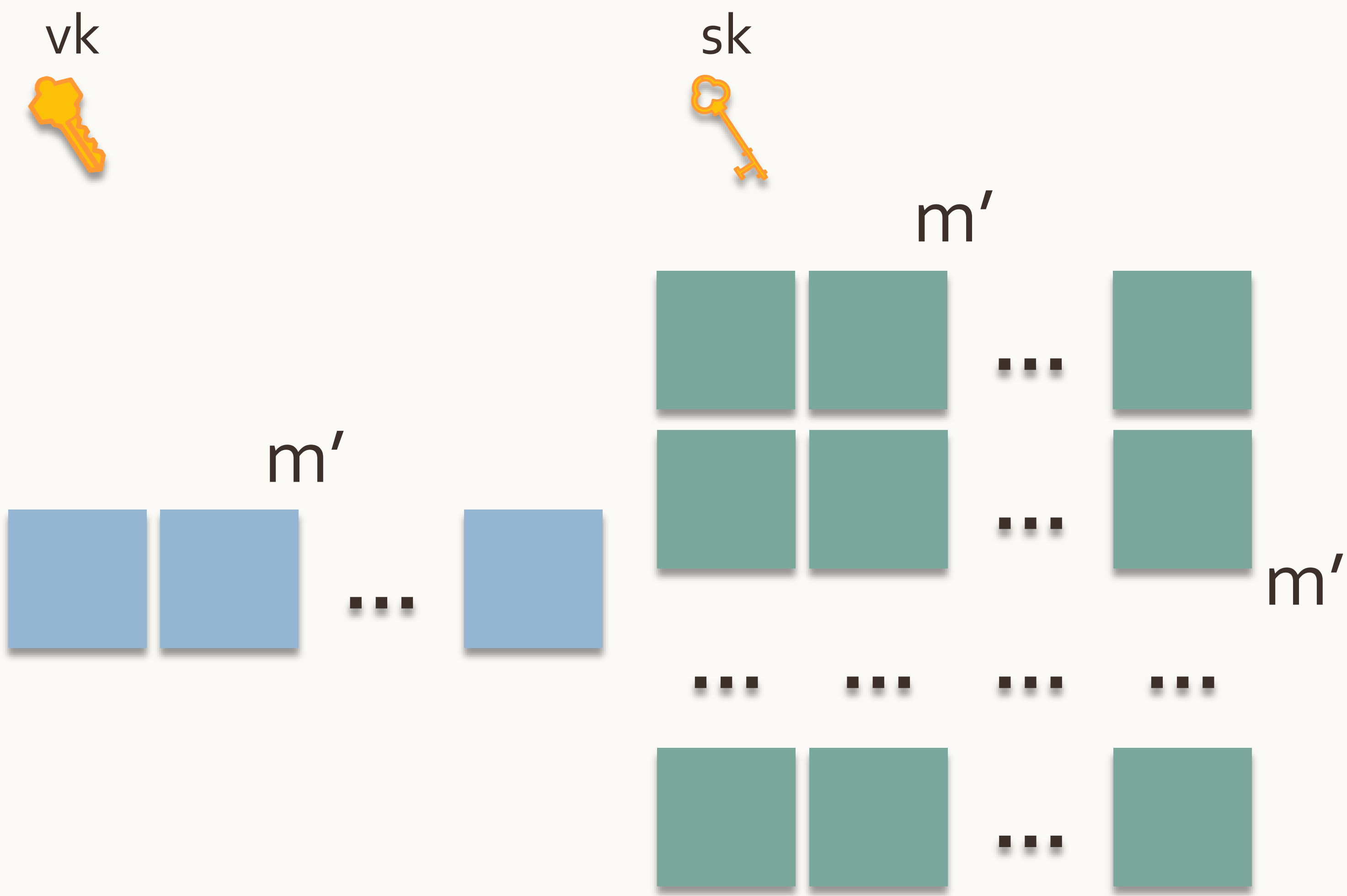


Our algorithm

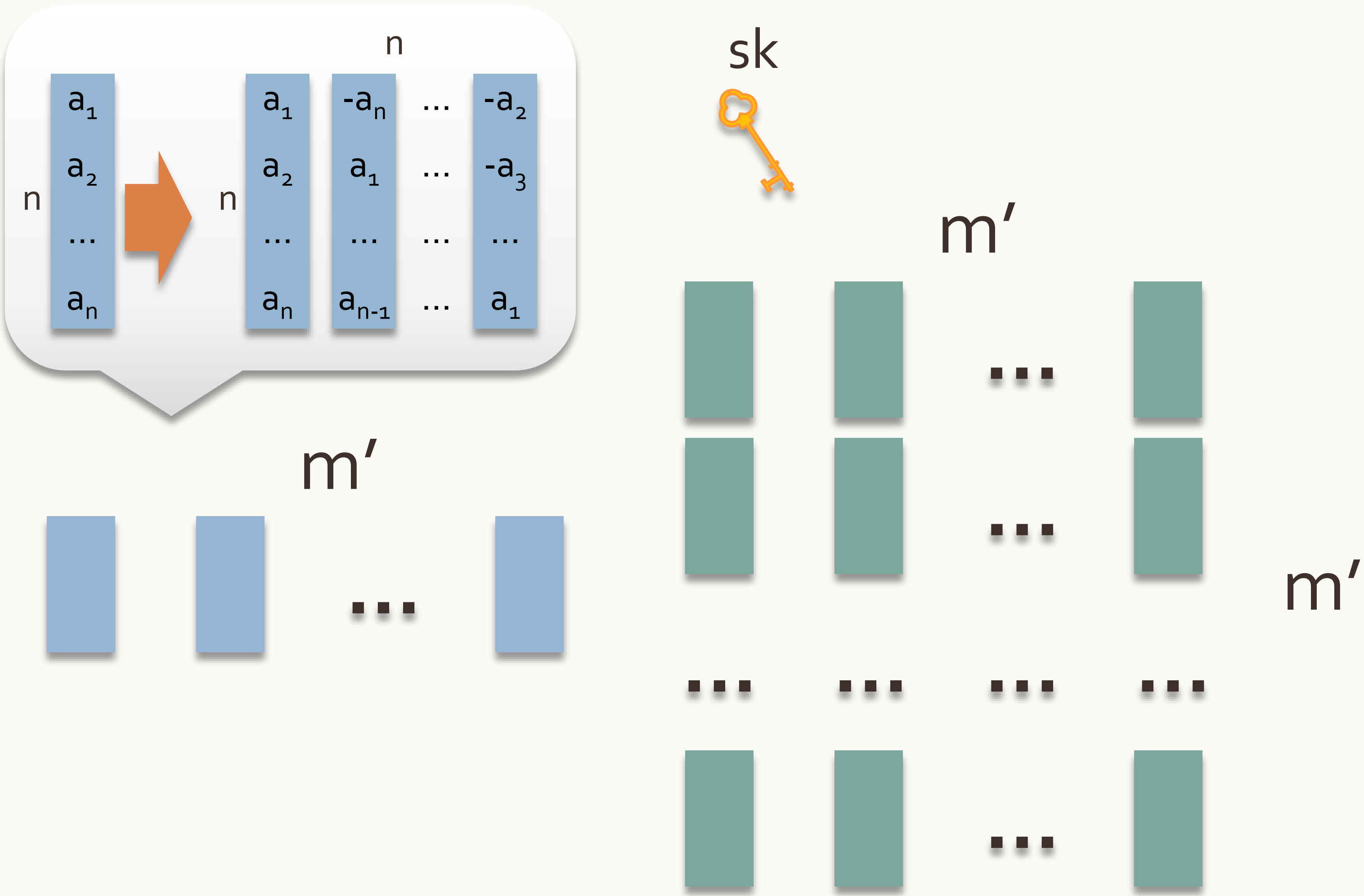
- Compose **A** and **S**



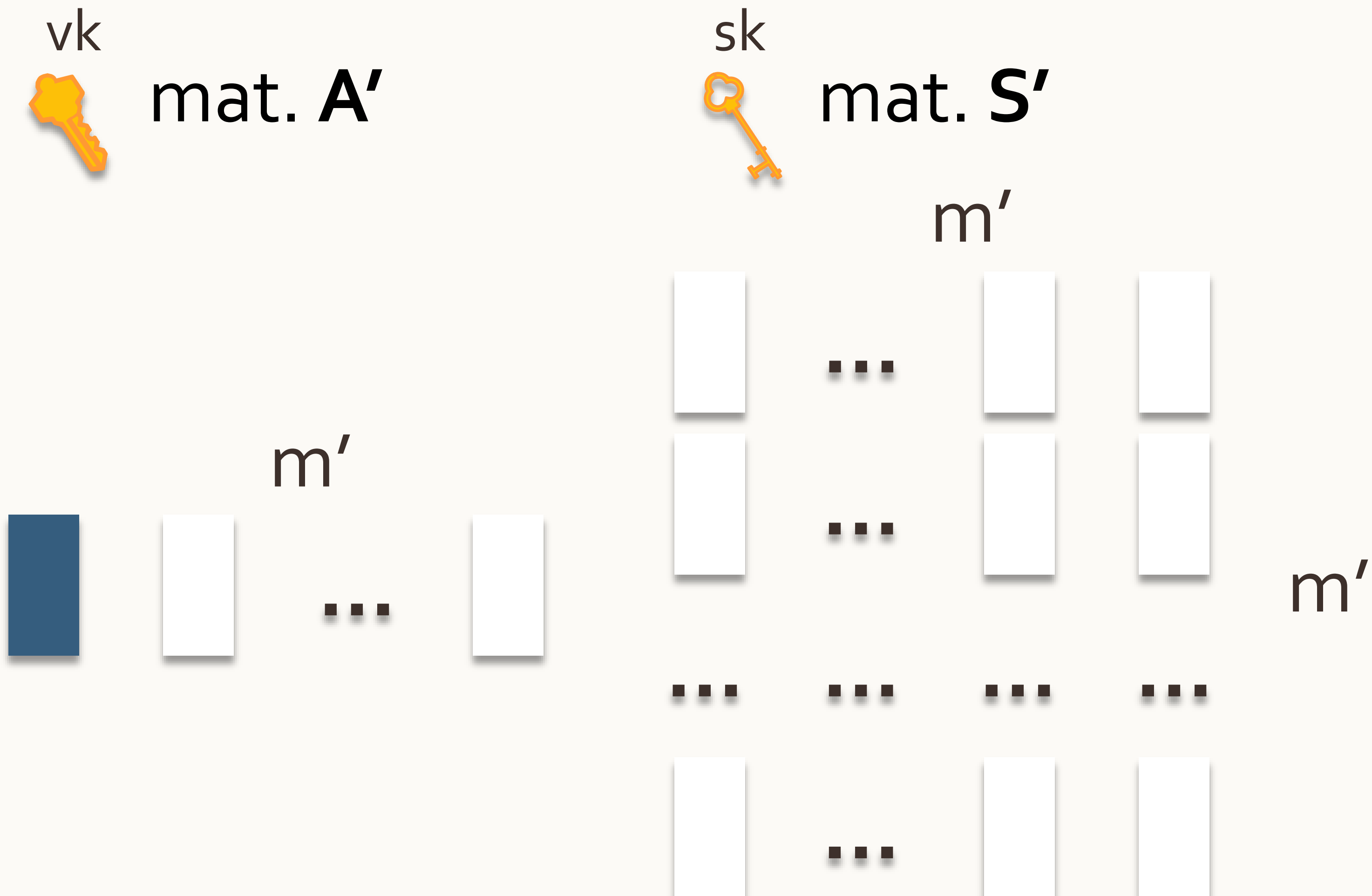
Our algorithm



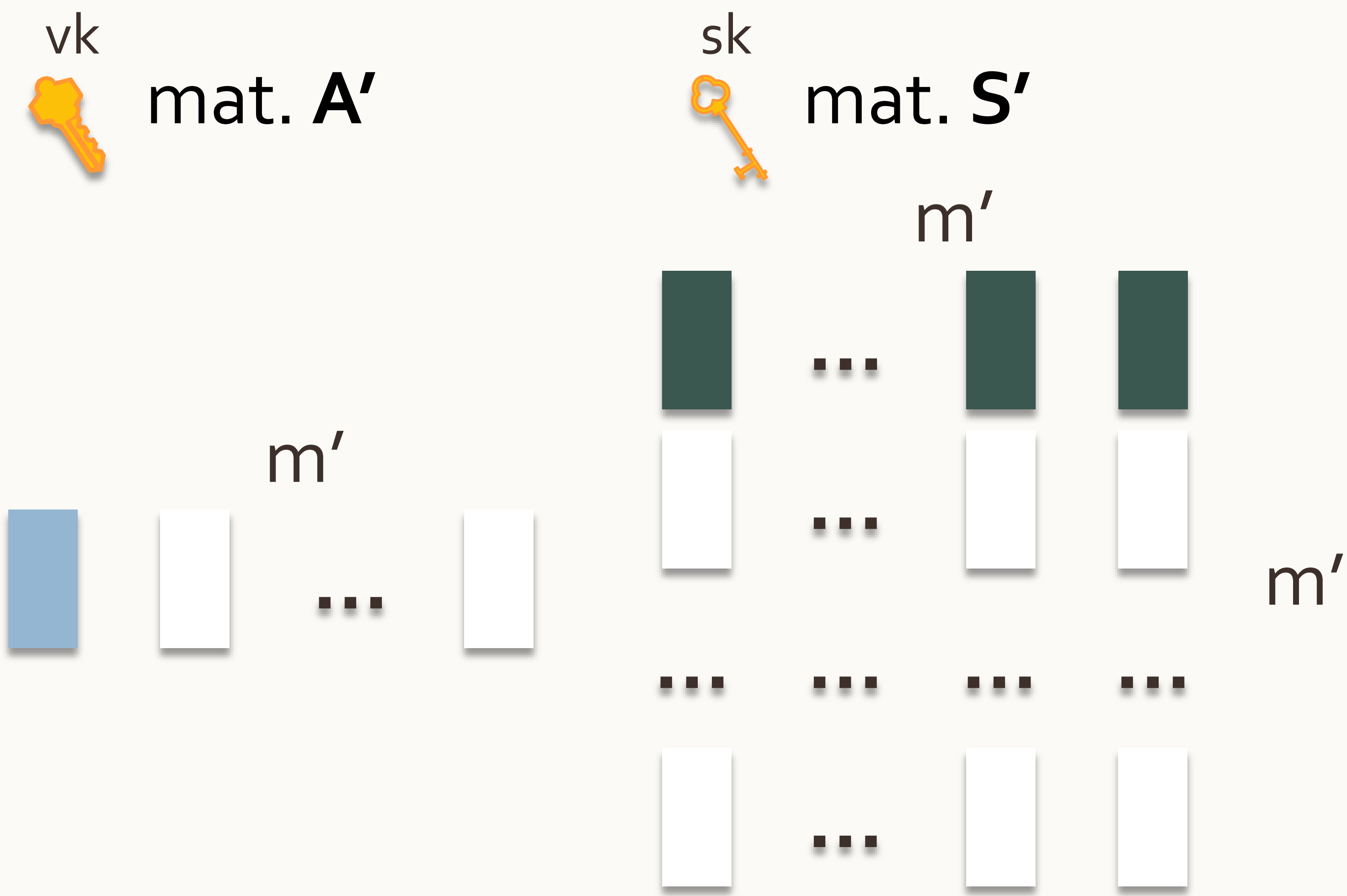
Our algorithm



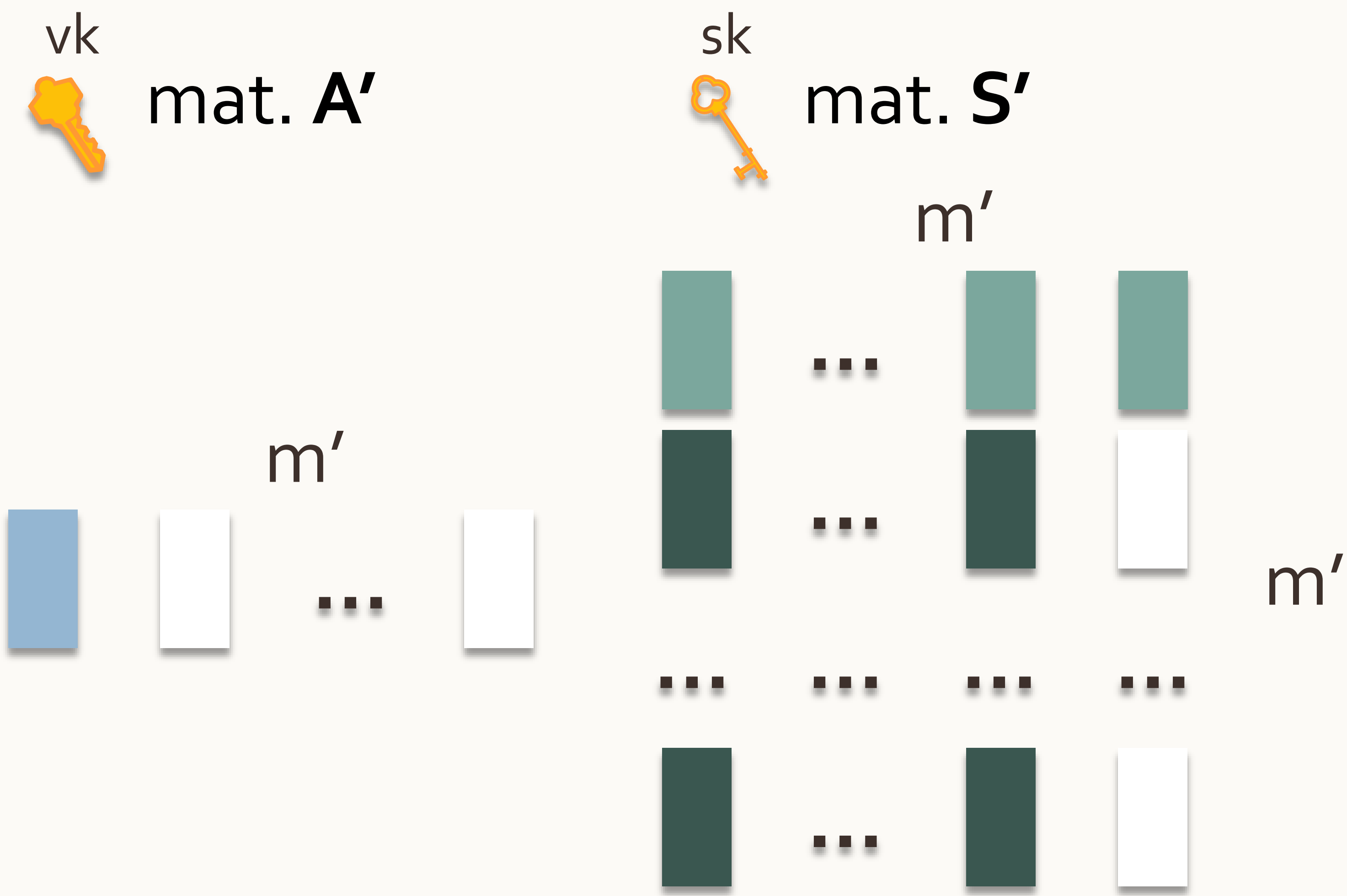
Our algorithm



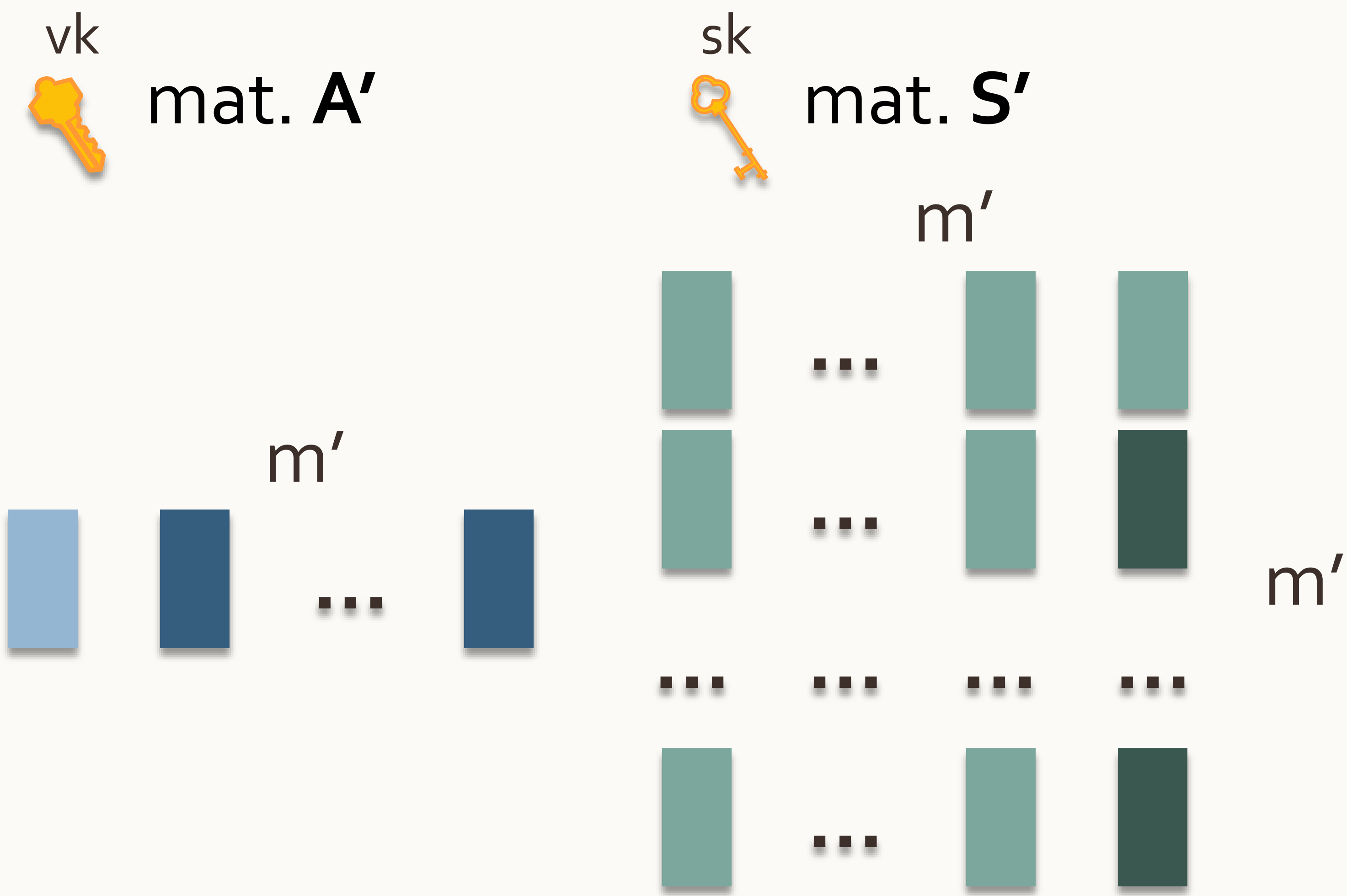
Our algorithm



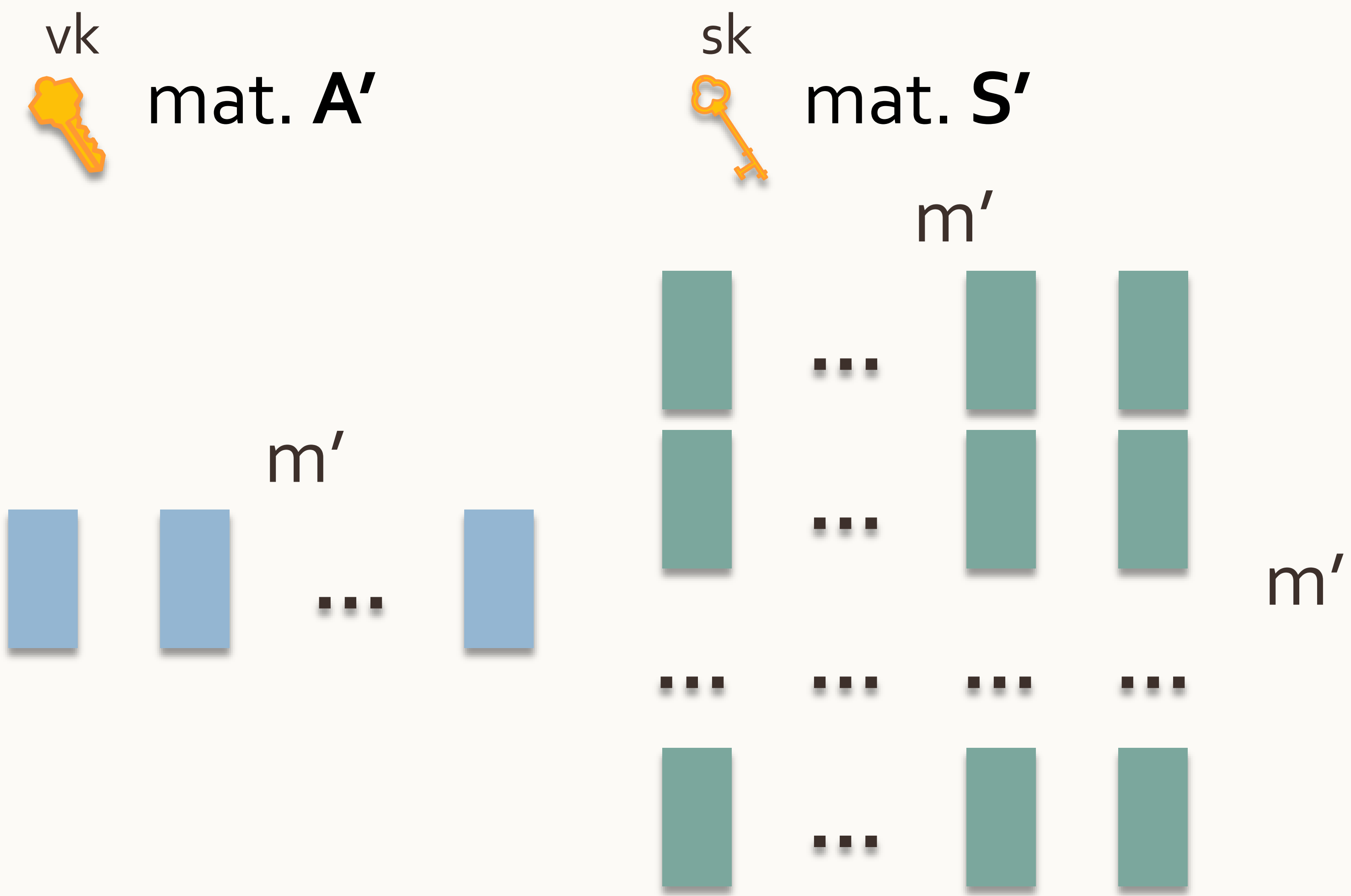
Our algorithm



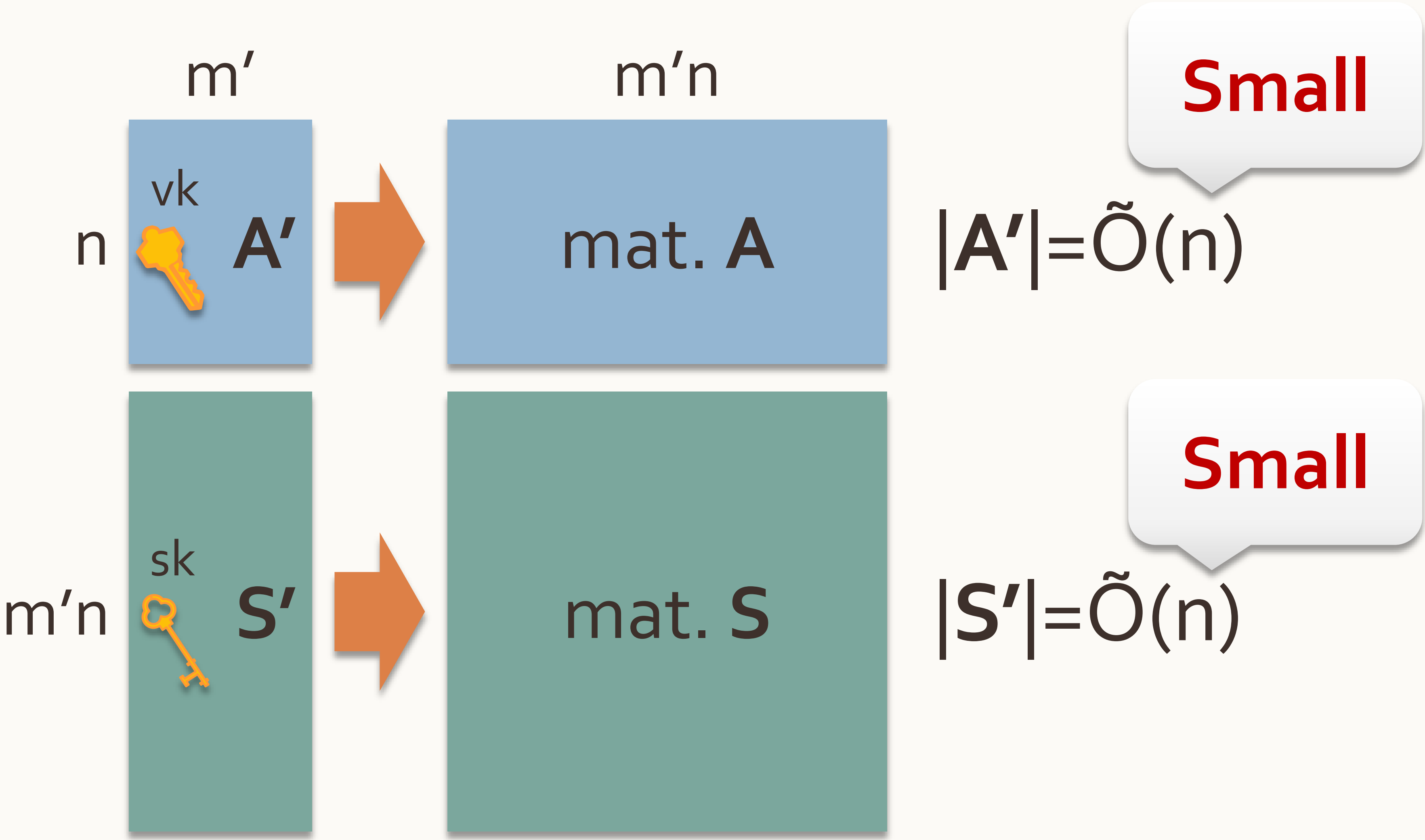
Our algorithm



Our algorithm



Results



Agenda

- Signature schemes
- Lattice problems
- The GPV signature scheme
  - Lattice-based hash functions
  - Ajtai's algorithm
- Our scheme
  - Ideal-lattice-based hash functions
  - Our algorithm
- Comparison GPV and ours

Comparison

Gentry, Peikert, Vaikuntanathan (2008)	Ours
Signature Scheme	Sginature Scheme
Based on **Lattices**	... on **Ideal Lattices**
Large vk and sk. **$\tilde{O}(n^2)$**	Small vk and sk. **$\tilde{O}(n)$**
n=256, **|vk|≈1MB**	n=256, **|vk|≈15kB**

References

- [GPV08]: Gentry, Peikert, and Vaikuntanathan (STOC ‘08)
  Trapdoors for Hard Lattices and New Cryptographic Constructions
- [A96]: Ajtai (STOC ‘96)
  Generating Hard Instances of Lattice Problems
- [A99]: Ajtai (ICALP ‘99)
  Generating Hard Instances of the Short Basis Problem
- [LM06]: Lyubashevsky and Micciancio (ICALP ’06)
  Generalized Compact Knapsacks are Collision Resistant