MPSign: A Signature from Small-Secret Middle-Product Learning with Errors

Shi Bai
Dipayan Das
Ryo Hiromasa
Miruna Rosca
Amin Sakzad
Damien Stehlé
Ron Steinfeld
Zhenfei Zhang

What is this talk about?

A digital signature scheme whose security in the QROM relies on the hardness of solving ApproxSVP^f for many polynomials f.

Main ingredient:

A reduction from small secret PLWE^f to small secret MP-LWE which works for many f's.

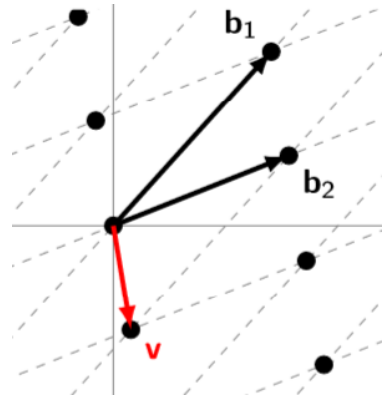
Overview

1. Background

2. Hardness of MP-LWE with small secrets

3. MPSign: our digital signature based on small secret MP-LWE

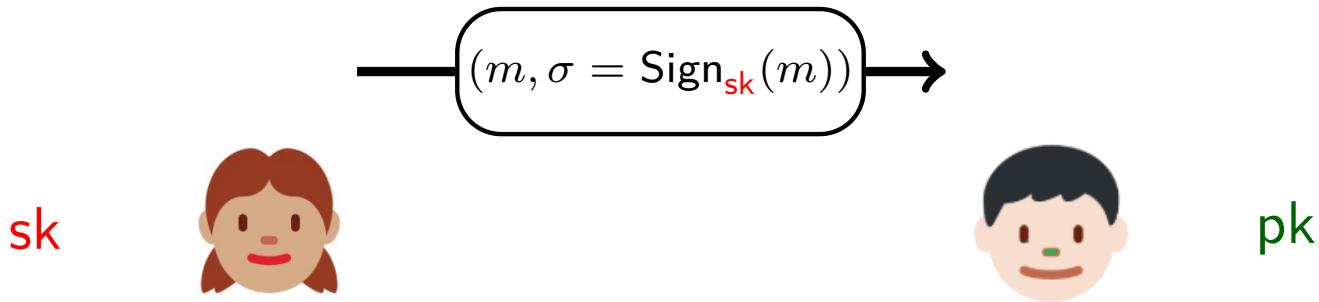
Background



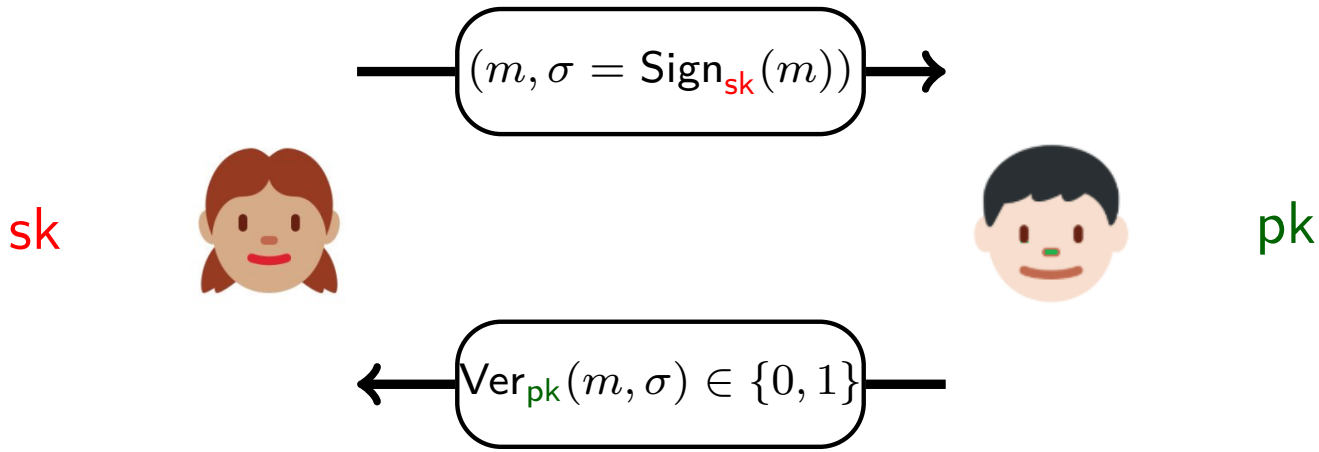
Digital signature DS = (Gen, Sign, Ver)

sk   pk

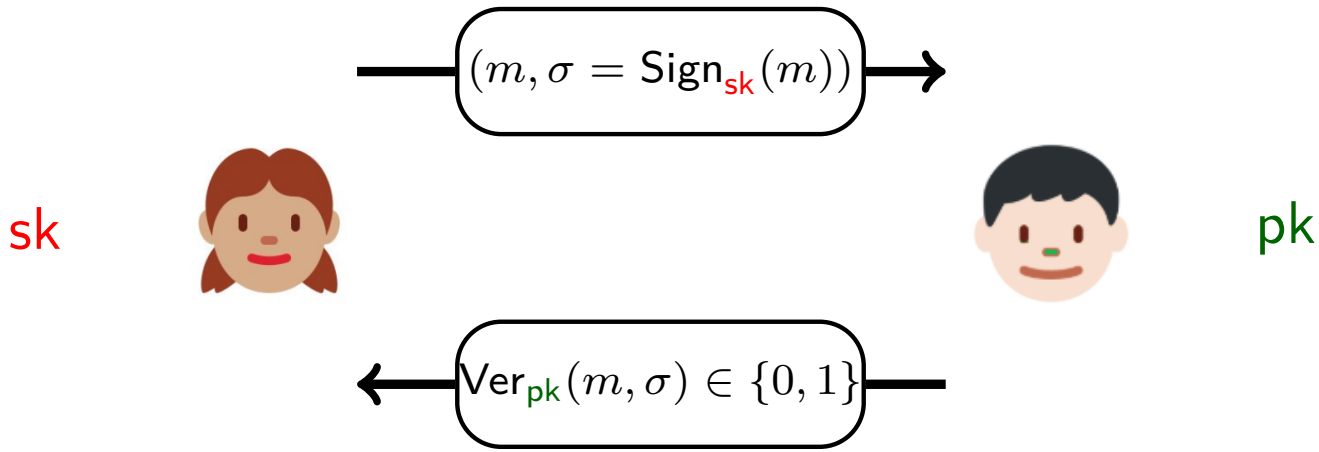
Digital signature DS = (Gen, Sign, Ver)



Digital signature DS = (Gen, Sign, Ver)

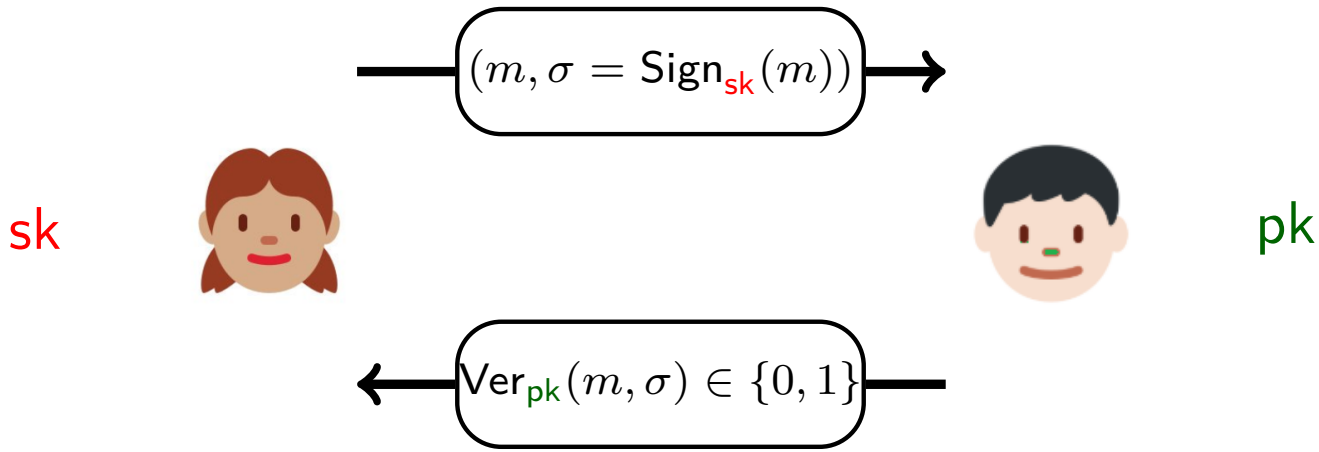


Digital signature DS = (Gen, Sign, Ver)



Correctness: $\mathsf{Ver}_{\mathsf{pk}}(m, \mathsf{Sign}_{\mathsf{sk}}(m)) = 1$ w.h.p.

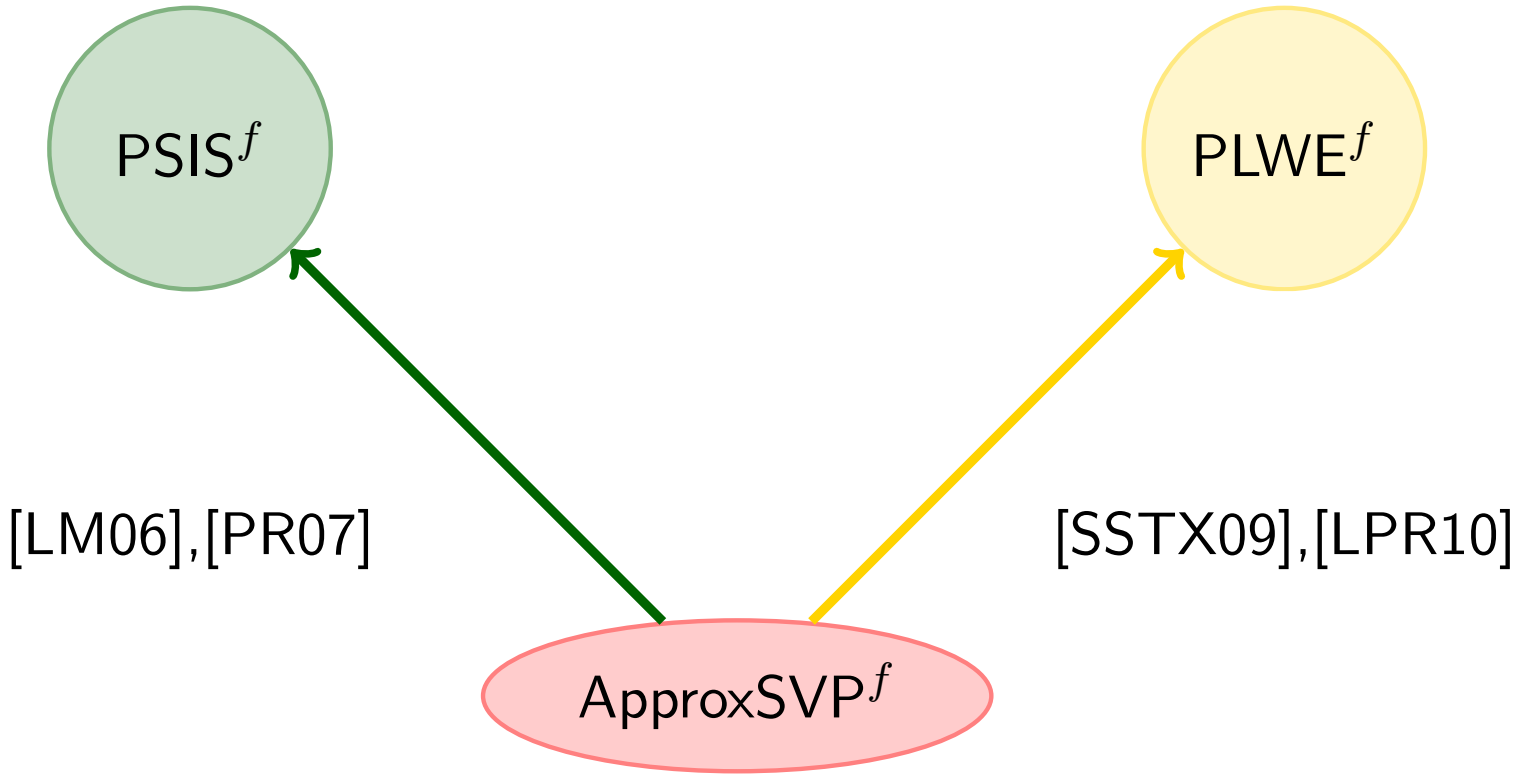
Digital signature DS = (Gen, Sign, Ver)



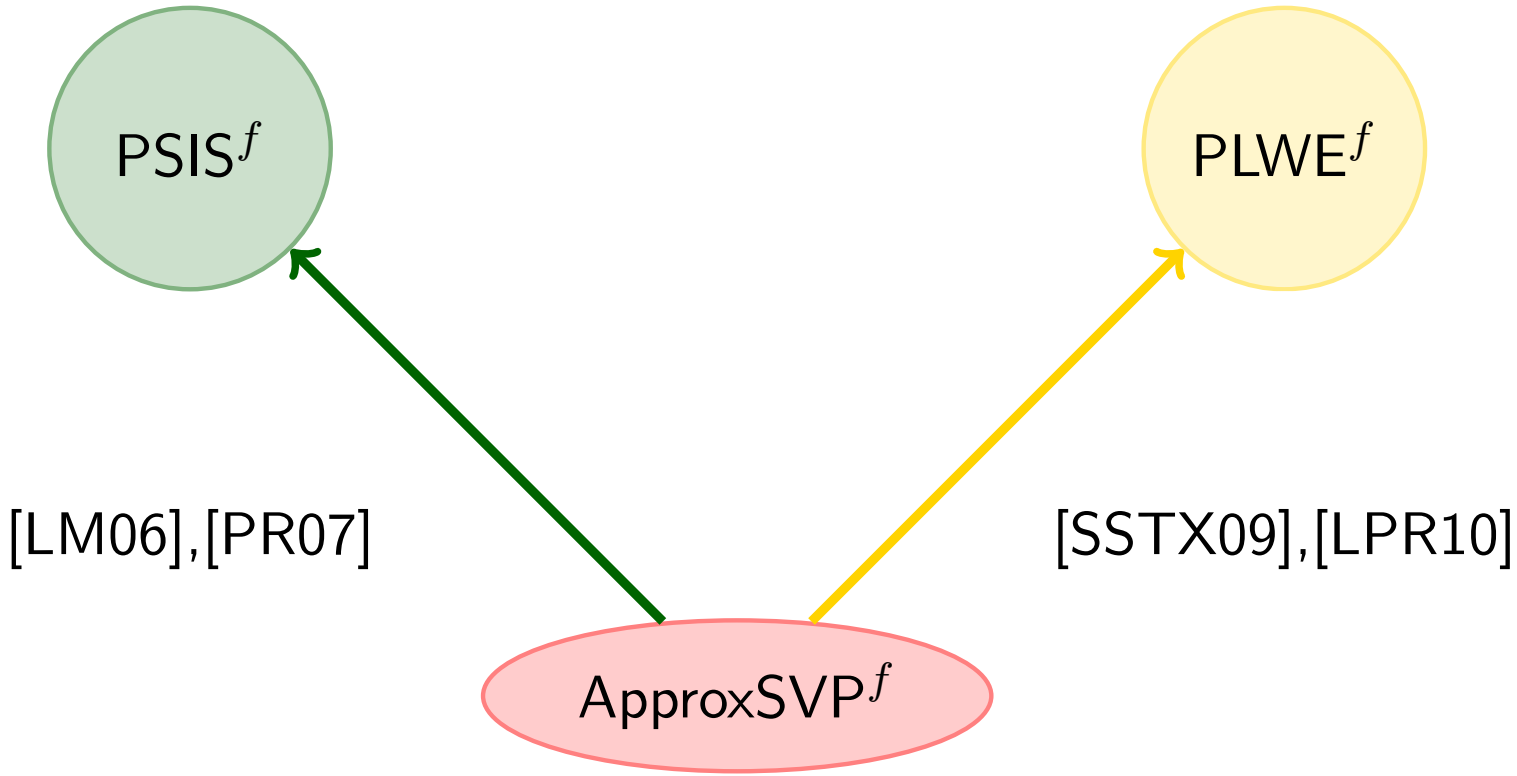
Correctness: $\mathsf{Ver}_{\mathsf{pk}}(m, \mathsf{Sign}_{\mathsf{sk}}(m)) = 1$ w.h.p.

ufCMA Security: DS is secure if no adversary, having access to many signatures, is able to produce a signature for a **new** message.

How to build lattice-based crypto?



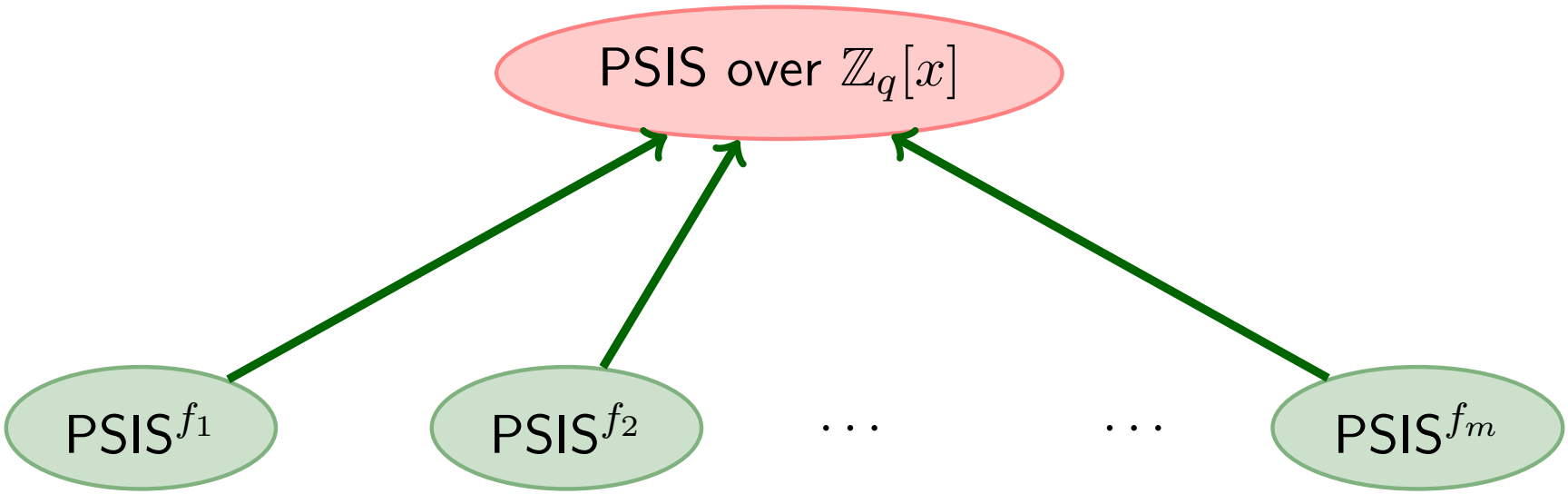
How to build lattice-based crypto?



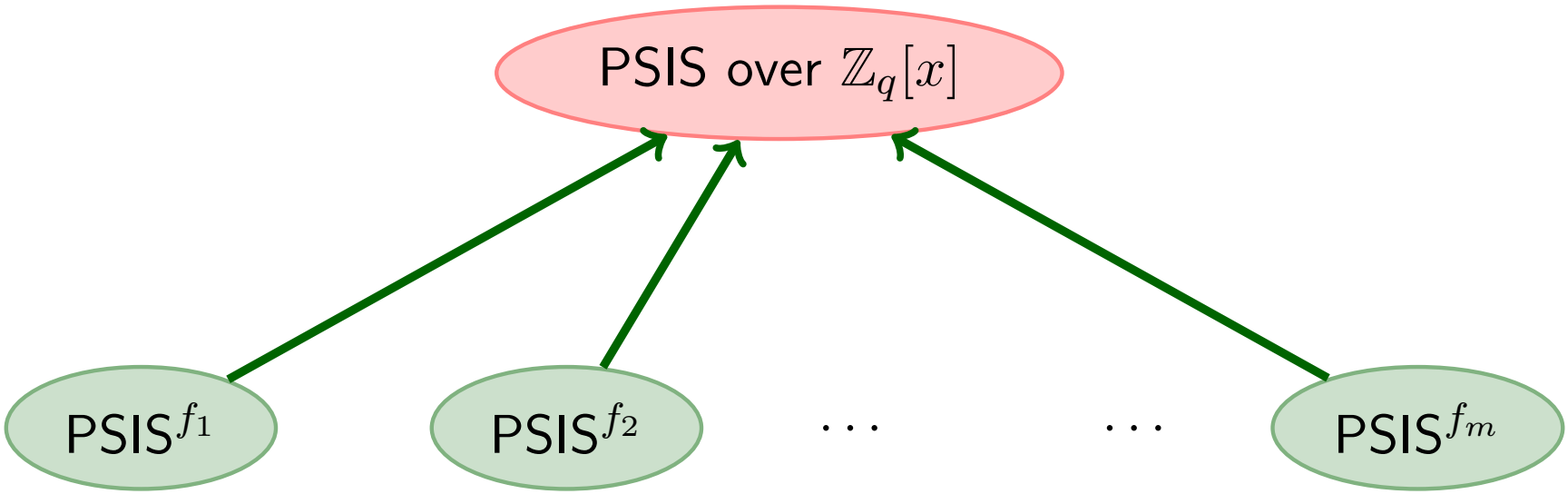
[CDPR16], [BBV+17], [CDW17], etc.

ApproxSVP^f is **easier** than ApproxSVP for some f's in some parameter regimes and setups.

[Lyu16]: A problem at least as hard as many PSIS^f

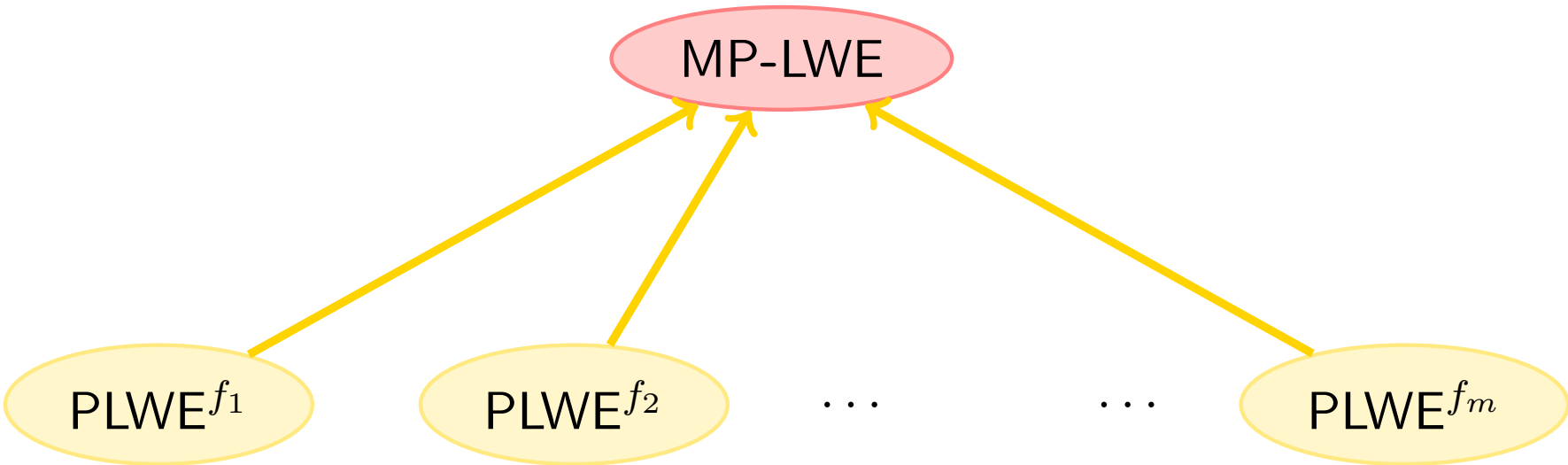


[Lyu16]: A problem at least as hard as many PSIS^f

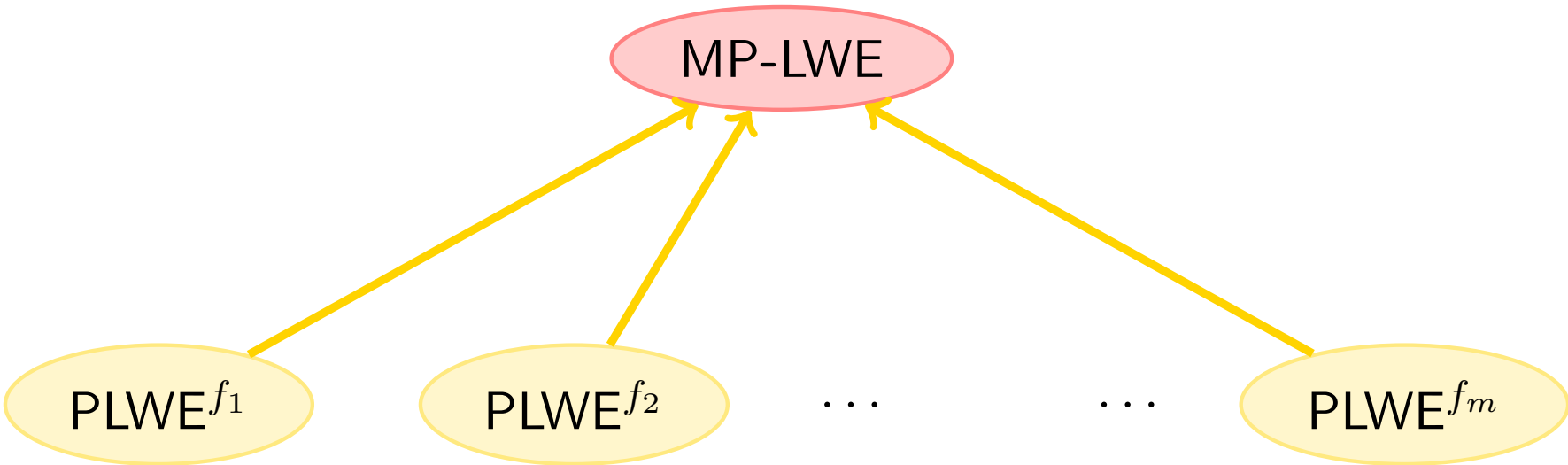


Application: digital signature scheme

[RSSS17]: A problem at least as hard as many PLWE^f



[RSSS17]: A problem at least as hard as many PLWE^f



Applications of MP-LWE

- public key encryption: [RSSS17], [SSZ18], [BBD+19]
- identity based encryption: [LVV19]

The PLWE^f and MP-LWE problems

f poly. of degree n

$$\mathsf{PLWE}^f_{q,\chi_1,\chi_2}$$

The PLWE^f and MP-LWE problems

f poly. of degree n

PLWE$^f_{q,\chi_1,\chi_2}$

P$^f_{q,\chi_1}(s)$ for $s \in \mathbb{Z}_q[x]/f$

- $a \hookleftarrow \mathsf{U}(\mathbb{Z}_q[x]/f)$ and $e \hookleftarrow \chi_1$
- return $(a, b = a \cdot s + e \bmod f)$

The PLWE^f and MP-LWE problems

f poly. of degree n

$\mathsf{PLWE}^f_{q,\chi_1,\chi_2}$

Distinguish between

$\mathsf{P}^f_{q,\chi_1}(s)$ for $s \in \mathbb{Z}_q[x]/f$

- $a \hookleftarrow \mathsf{U}(\mathbb{Z}_q[x]/f)$ and $e \hookleftarrow \chi_1$
- return $(a, b = a \cdot s + e \bmod f)$

and

$\mathsf{U}(\mathbb{Z}_q[x]/f \times \mathbb{R}_q[x]/f)$

The PLWE^f and MP-LWE problems

f poly. of degree n

$$\mathsf{PLWE}^f_{q,\chi_1,\chi_2}$$

Distinguish between

$\mathsf{P}^f_{q,\chi_1}(s)$ for $s \in \mathbb{Z}_q[x]/f$

- $a \hookleftarrow \mathsf{U}(\mathbb{Z}_q[x]/f)$ and $e \hookleftarrow \chi_1$
- return $(a, b = a \cdot s + e \bmod f)$

and

$$\mathsf{U}(\mathbb{Z}_q[x]/f \times \mathbb{R}_q[x]/f)$$

with non-negl. probability over the choice of $s \hookleftarrow \chi_2$.

The PLWE^f and MP-LWE problems

f poly. of degree n

PLWE$^f_{q,\chi_1,\chi_2}$

MP-LWE$^{n,d}_{q,\chi_1,\chi_2}$

Distinguish between

P$^f_{q,\chi_1}(s)$ for $s \in \mathbb{Z}_q[x]/f$

- $a \hookleftarrow \mathsf{U}(\mathbb{Z}_q[x]/f)$ and $e \hookleftarrow \chi_1$
- return $(a, b = a \cdot s + e \bmod f)$

and

$\mathsf{U}(\mathbb{Z}_q[x]/f \times \mathbb{R}_q[x]/f)$

with non-negl. probability over the choice of $s \hookleftarrow \chi_2$.

The PLWE^f and MP-LWE problems

f poly. of degree n

$\mathsf{PLWE}^f_{q,\chi_1,\chi_2}$	$\mathsf{MP\text{-}LWE}^{n,d}_{q,\chi_1,\chi_2}$

Distinguish between

$\mathsf{P}^f_{q,\chi_1}(s)$ for $s \in \mathbb{Z}_q[x]/f$	$\mathsf{MP}^{n,d}_{q,\chi_1}(s)$ for $s \in \mathbb{Z}_q^{<n+d-1}[x]$
• $a \hookleftarrow \mathsf{U}(\mathbb{Z}_q[x]/f)$ and $e \hookleftarrow \chi_1$ • return $(a, b = a \cdot s + e \bmod f)$	• $a \hookleftarrow \mathsf{U}(\mathbb{Z}_q^{<n}[x])$ and $e \hookleftarrow \chi_1$ • return $(a, b = a \odot_d s + e)$

and

$\mathsf{U}(\mathbb{Z}_q[x]/f \times \mathbb{R}_q[x]/f)$

with non-negl. probability over the choice of $s \hookleftarrow \chi_2$.

The PLWE^f and MP-LWE problems

f poly. of degree n

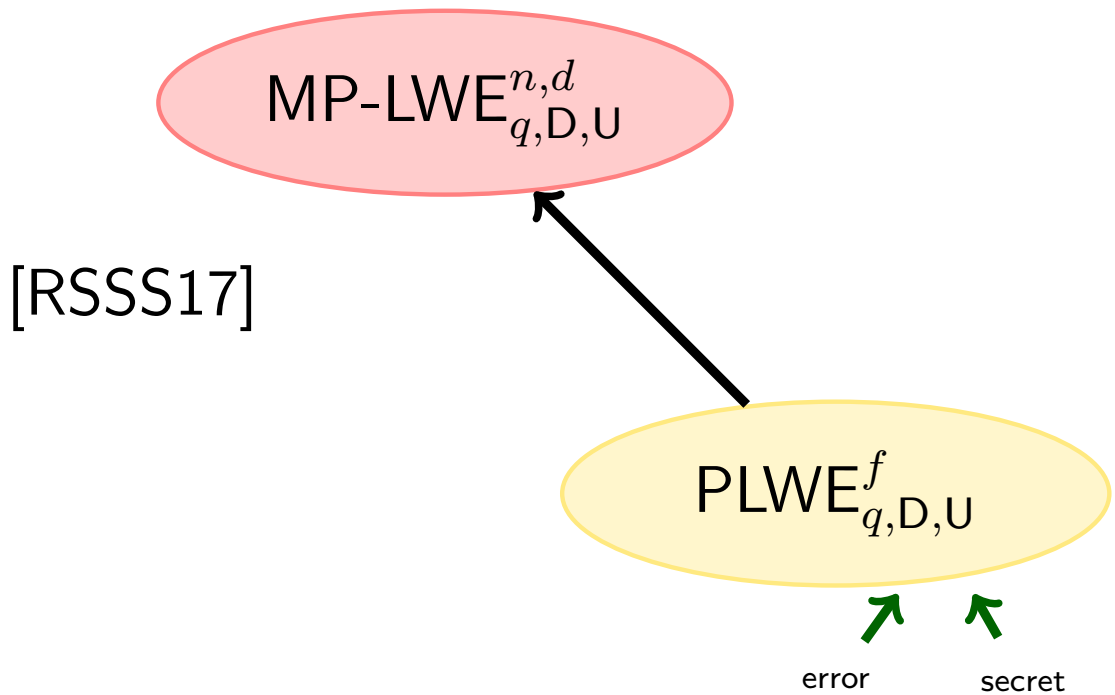
$\mathsf{PLWE}^f_{q,\chi_1,\chi_2}$	$\mathsf{MP\text{-}LWE}^{n,d}_{q,\chi_1,\chi_2}$
Distinguish between	Distinguish between
$\mathsf{P}^f_{q,\chi_1}(s)$ for $s \in \mathbb{Z}_q[x]/f$	$\mathsf{MP}^{n,d}_{q,\chi_1}(s)$ for $s \in \mathbb{Z}_q^{<n+d-1}[x]$
• $a \hookleftarrow \mathsf{U}(\mathbb{Z}_q[x]/f)$ and $e \hookleftarrow \chi_1$ • return $(a, b = a \cdot s + e \bmod f)$	• $a \hookleftarrow \mathsf{U}(\mathbb{Z}_q^{<n}[x])$ and $e \hookleftarrow \chi_1$ • return $(a, b = a \odot_d s + e)$
and	and
$\mathsf{U}(\mathbb{Z}_q[x]/f \times \mathbb{R}_q[x]/f)$	$\mathsf{U}(\mathbb{Z}_q^{<n}[x] \times \mathbb{R}_q^{<d}[x])$

with non-negl. probability over the choice of $s \hookleftarrow \chi_2$.

Hardness of MP-LWE with small secrets

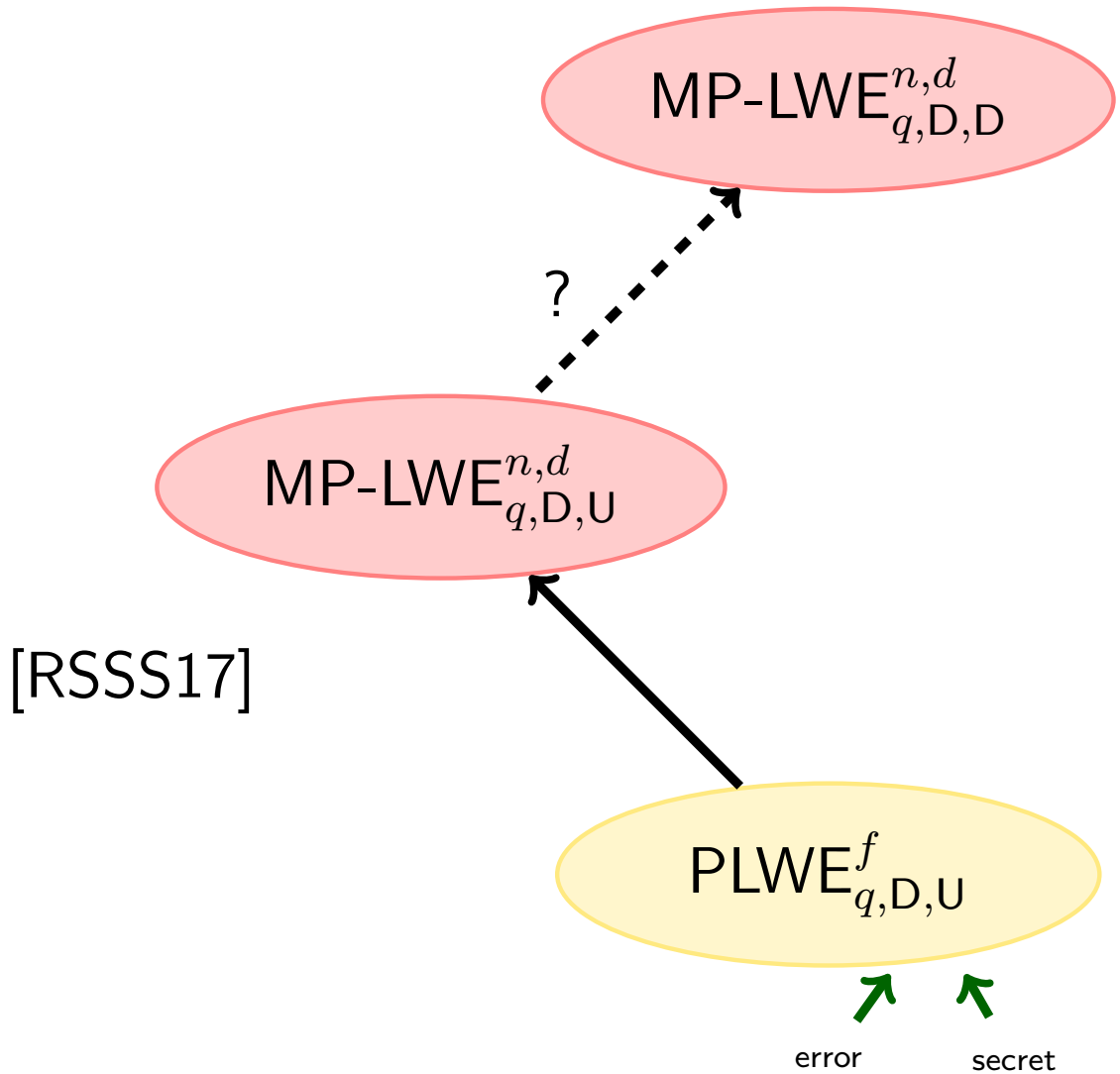
Towards the hardness of MP-LWE with small secret

* D: distribution which produces small elements w.h.p
* U: uniform distribution



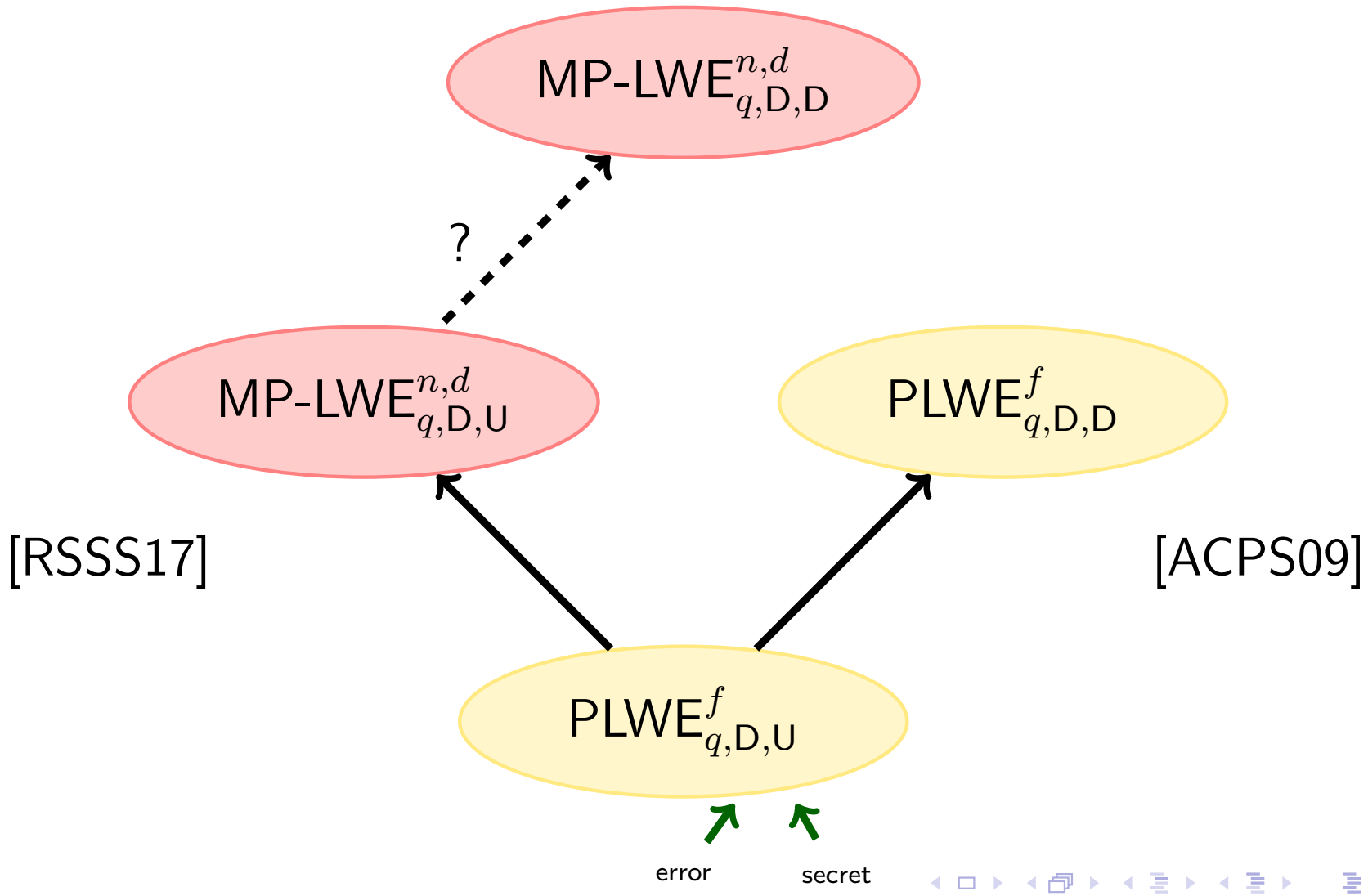
Towards the hardness of MP-LWE with small secret

* D: distribution which produces small elements w.h.p
* U: uniform distribution



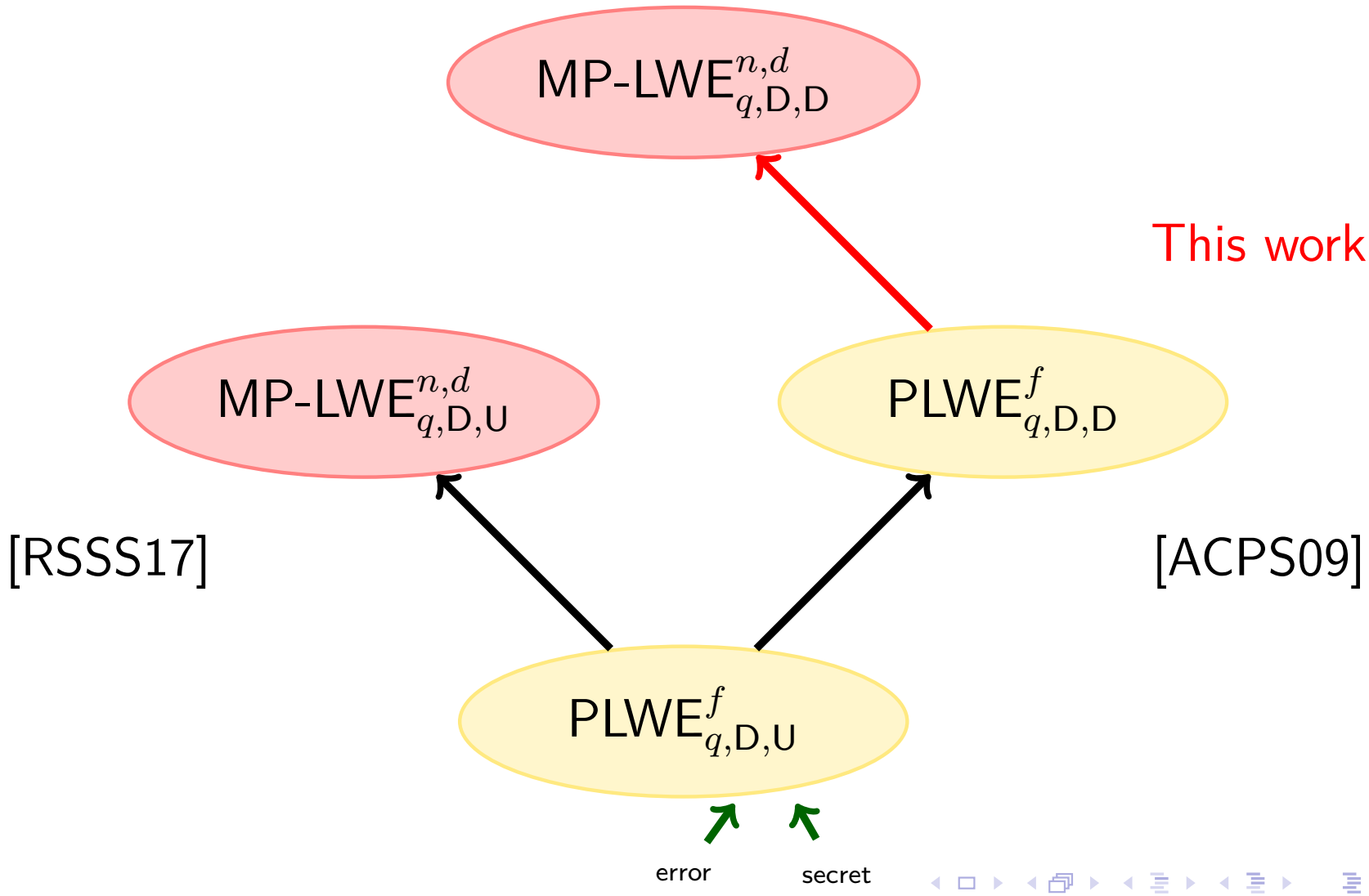
Towards the hardness of MP-LWE with small secret

* D: distribution which produces small elements w.h.p
* U: uniform distribution



Towards the hardness of MP-LWE with small secret

* D: distribution which produces small elements w.h.p
* U: uniform distribution



From PLWE^f to MP-LWE for many f's

* $f \in \mathbb{Z}[x]$ of degree n, $d \leq n$
* $\mathsf{D}_{\mathbb{R},\sigma}$: Gaussian on $\mathbb{R}$ with standard deviation σ
* $\mathsf{D}_{\mathbb{Z},\sigma}$: Gaussian on $\mathbb{Z}$ with standard deviation σ

[RSSS17]	MP-LWE$^{n,d}_{q,\chi_1,\chi_2}$	PLWE$^{f}_{q,\chi_1,\chi_2}$
χ_1	$\mathsf{D}_{\mathbb{R}^d,\alpha' q}$	$\mathsf{D}_{\mathbb{R}^n,\alpha q}$
χ_2	$\mathsf{U}(\mathbb{Z}_q^{n+d-1})$	$\mathsf{U}(\mathbb{Z}_q^{n})$

This work	MP-LWE$^{n,d}_{q,\chi_1,\chi_2}$	PLWE$^{f}_{q,\chi_1,\chi_2}$
χ_1	$\mathsf{D}_{\mathbb{Z}^d,\alpha'' q}$	$\mathsf{D}_{\mathbb{Z}^n,\alpha q}$
χ_2	$\mathsf{D}_{\mathbb{Z}^{n+d-1},\alpha' q}$	$\mathsf{D}_{\mathbb{Z}^n,\alpha q}$

Recall [RSSS17]

$$\mathsf{Rot}_f(b) = \mathsf{Rot}_f(a) \times \mathsf{Rot}_f(s) + \mathsf{Rot}_f(e)$$

Recall [RSSS17]

$$\mathsf{Rot}_f(b) = \mathsf{Rot}_f(a) \times \mathsf{Rot}_f(s) + \mathsf{Rot}_f(e)$$

Take first column

$$M_f \, b = \mathsf{Rot}_f(a) \times M_f \, s + M_f \, e$$

Recall [RSSS17]

$$\mathsf{Rot}_f(b) = \mathsf{Rot}_f(a) \times \mathsf{Rot}_f(s) + \mathsf{Rot}_f(e)$$

Take first column

$$M_f \, b = \mathsf{Rot}_f(a) \times M_f \, s + M_f \, e$$

Decompose $\mathsf{Rot}_f(a)$

$$b' = \mathsf{Toep}(a) \, \mathsf{Rot}_f(1) \times M_f \, s + M_f \, e$$

Recall [RSSS17]

$$\mathsf{Rot}_f(b) = \mathsf{Rot}_f(a) \times \mathsf{Rot}_f(s) + \mathsf{Rot}_f(e)$$

Take first column

$$M_f \; b = \mathsf{Rot}_f(a) \times M_f \; s + M_f \; e$$

Decompose $\mathsf{Rot}_f(a)$

$$b' = \mathsf{Toep}(a) \; \mathsf{Rot}_f(1) \times M_f \; s + M_f \; e$$

Rename

$$b' = \mathsf{Toep}(a) \times s' + e'$$

From small secret PLWE^f to small secret MP-LWE

$$M_f \quad e \quad + \quad \overline{e}$$

From small secret PLWE^f to small secret MP-LWE

$$M_f \quad e \quad + \quad \overline{e}$$

$$\mathsf{D}_{\mathbb{Z},\alpha} + \mathsf{D}_{\mathbb{Z},\beta} \approx \mathsf{D}_{\mathbb{Z},\gamma}$$

From small secret PLWE^f to small secret MP-LWE

$$M_f \quad e \quad + \quad \overline{e}$$

$$\mathsf{D}_{\mathbb{Z},\alpha} + \mathsf{D}_{\mathbb{Z},\beta} \approx \mathsf{D}_{\mathbb{Z},\gamma}$$

We need a lower bound on the smallest singular value of M_f.

From small secret PLWE^f to small secret MP-LWE

$$M_f \quad e \quad + \quad \overline{e}$$

$$\mathsf{D}_{\mathbb{Z},\alpha} + \mathsf{D}_{\mathbb{Z},\beta} \approx \mathsf{D}_{\mathbb{Z},\gamma}$$

We need a lower bound on the smallest singular value of M_f.

- more restrictive family of f's

$$\mathsf{M}_f = \left(\begin{array}{ccc|ccc} * & 0 & 0 & * & * & * \\ 0 & * & 0 & 0 & * & * \\ 0 & 0 & * & 0 & 0 & * \\ \hline 0 & 0 & 0 & * & 0 & 0 \\ 0 & 0 & 0 & 0 & * & 0 \\ 0 & 0 & 0 & 0 & 0 & * \end{array}\right)$$

From small secret PLWE^f to small secret MP-LWE

$$M_f \quad e \quad + \quad \overline{e}$$

$$\mathsf{D}_{\mathbb{Z},\alpha} + \mathsf{D}_{\mathbb{Z},\beta} \approx \mathsf{D}_{\mathbb{Z},\gamma}$$

We need a lower bound on the smallest singular value of M_f.

- more restrictive family of f's
- larger noise amplification

$$\mathsf{M}_f = \left(\begin{array}{ccc|ccc} * & 0 & 0 & * & * & * \\ 0 & * & 0 & 0 & * & * \\ 0 & 0 & * & 0 & 0 & * \\ \hline 0 & 0 & 0 & * & 0 & 0 \\ 0 & 0 & 0 & 0 & * & 0 \\ 0 & 0 & 0 & 0 & 0 & * \end{array}\right)$$

From small secret PLWE^f to small secret MP-LWE

$$M_f \quad e \quad + \quad \overline{e}$$

$$\mathsf{D}_{\mathbb{Z},\alpha} + \mathsf{D}_{\mathbb{Z},\beta} \approx \mathsf{D}_{\mathbb{Z},\gamma}$$

We need a lower bound on the smallest singular value of M_f.

- more restrictive family of f's
- larger noise amplification
- α is related to the family

$$\mathsf{M}_f = \left(\begin{array}{ccc|ccc} * & 0 & 0 & * & * & * \\ 0 & * & 0 & 0 & * & * \\ 0 & 0 & * & 0 & 0 & * \\ \hline 0 & 0 & 0 & * & 0 & 0 \\ 0 & 0 & 0 & 0 & * & 0 \\ 0 & 0 & 0 & 0 & 0 & * \end{array}\right)$$

Digital signature based on MP-LWE

Identification scheme ID = (IGen, P, V)

sk   vk

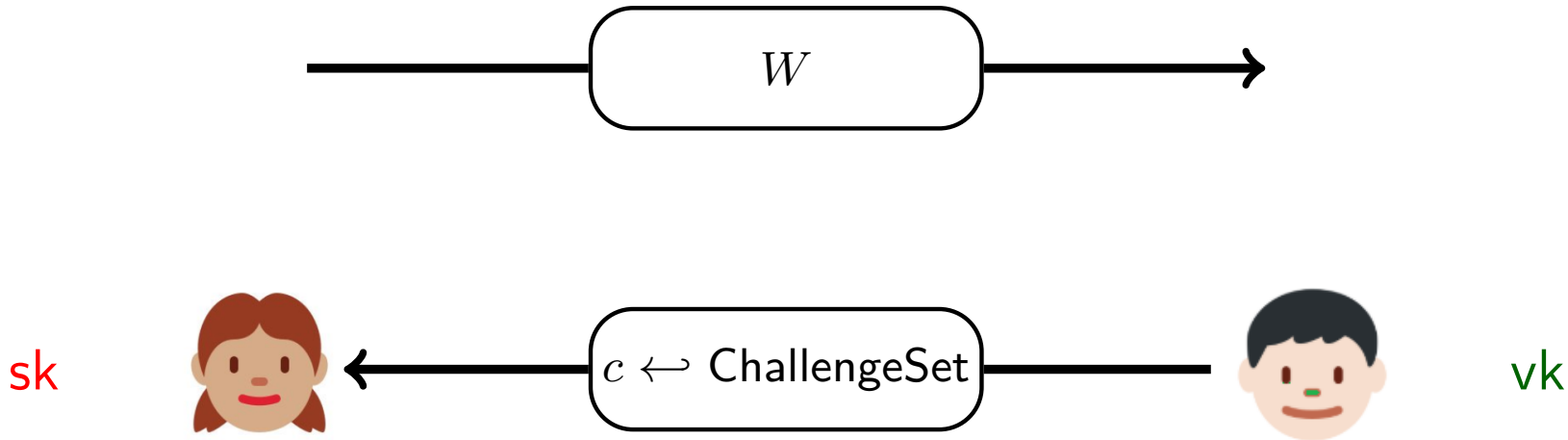
Identification scheme ID = (IGen, P, V)

sk   vk

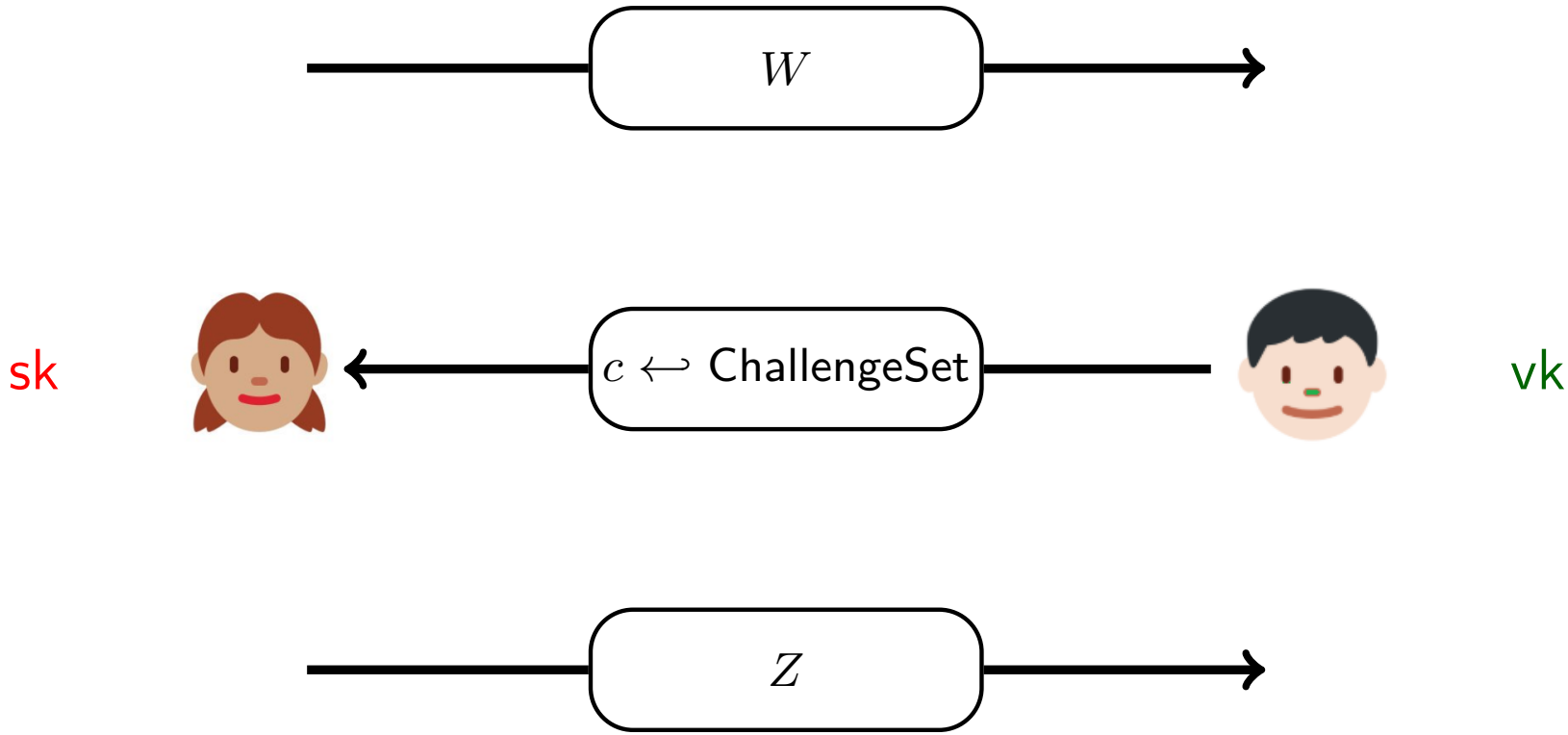
Identification scheme ID = (IGen, P, V)

sk   vk

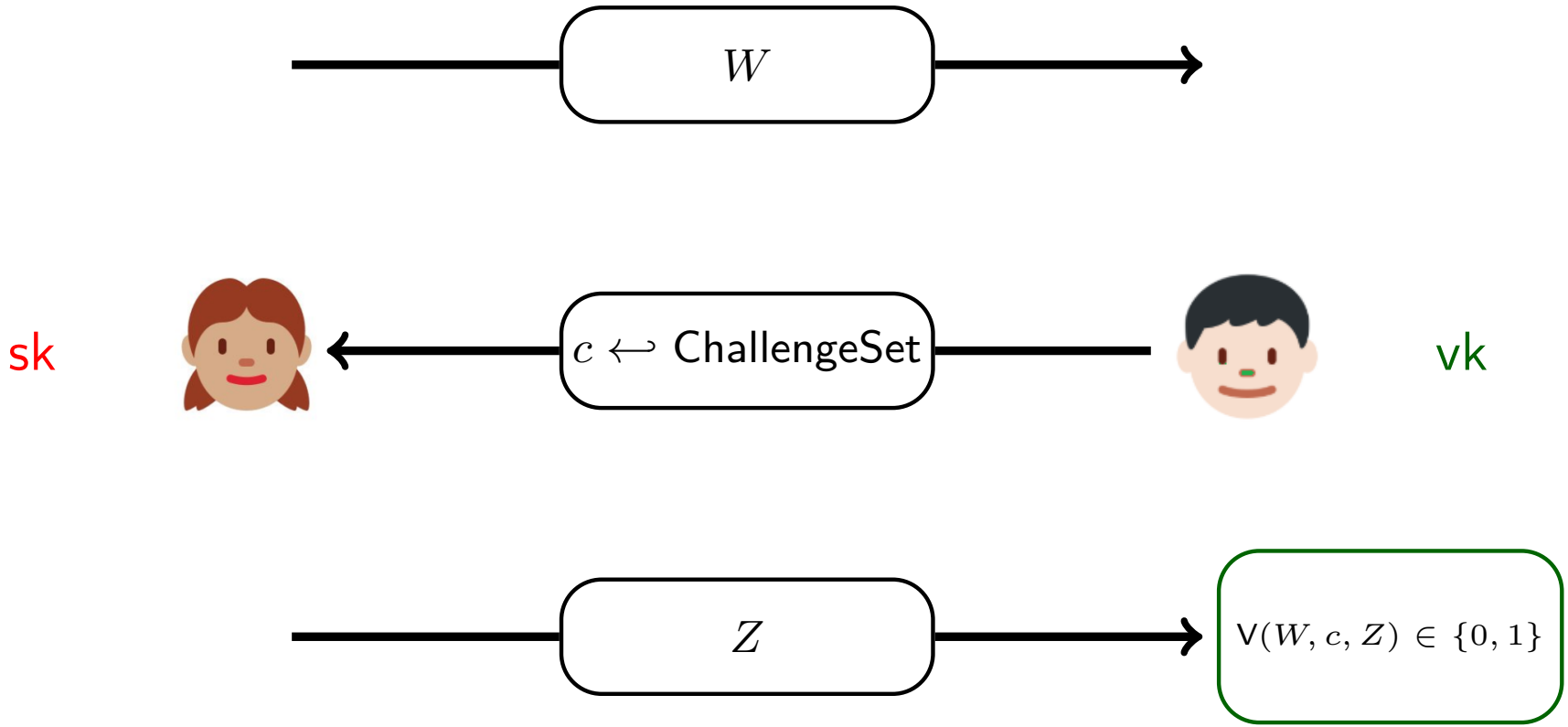
Identification scheme ID $= (\mathsf{IGen}, \mathsf{P}, \mathsf{V})$



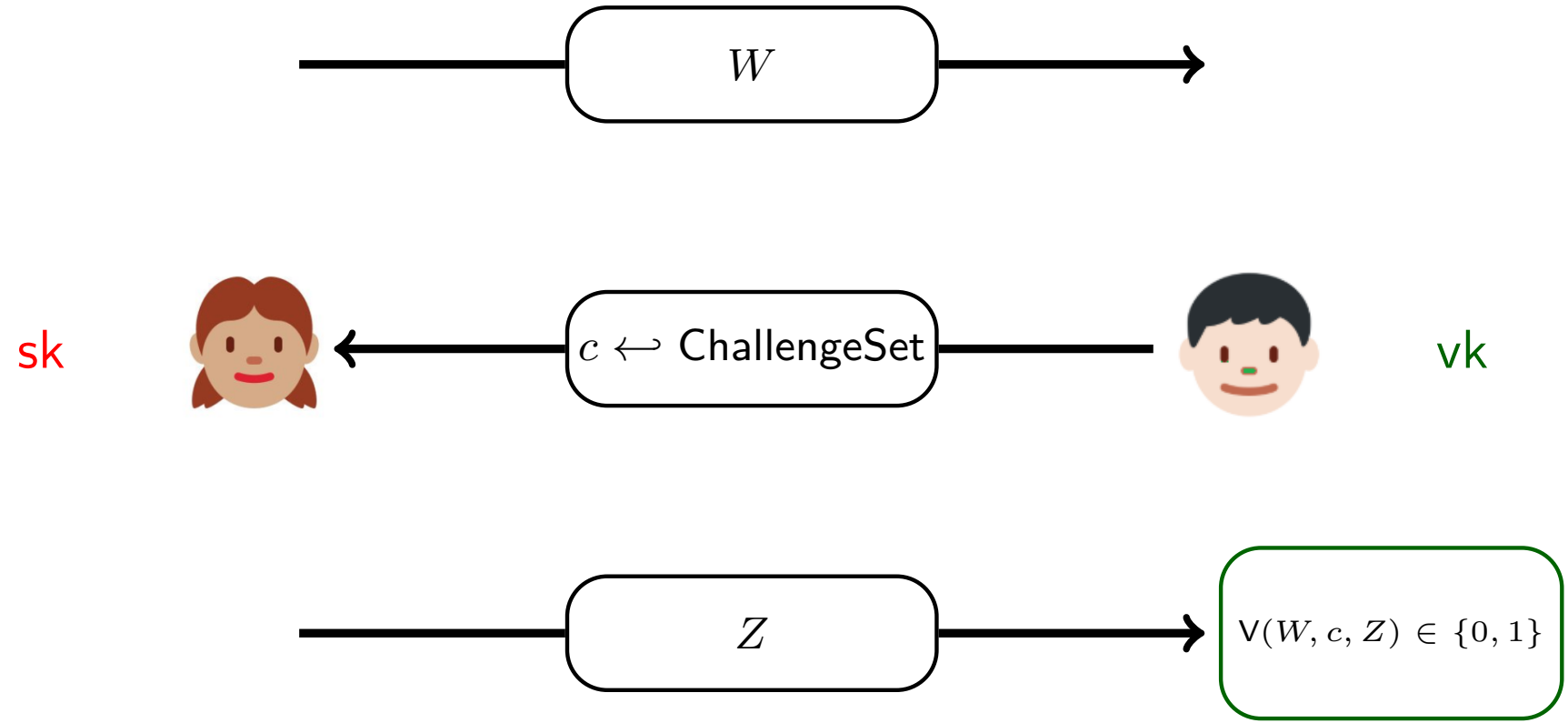
Identification scheme ID $= (\mathsf{IGen}, \mathsf{P}, \mathsf{V})$



Identification scheme ID $= (\mathsf{IGen}, \mathsf{P}, \mathsf{V})$



Identification scheme ID = (IGen, P, V)



Security: ID is secure if no adversary having access to multiple transcripts (W,c,Z) is able to fool the verifier.

Our identification scheme based on MP-LWE

(s, e) 

 $(a, b = a \odot s + e)$

Our identification scheme based on MP-LWE

(s, e) 

 $(a, b = a \odot s + e)$

$y_1,\ y_2$ small

$W = a \odot y_1 + y_2$

Our identification scheme based on MP-LWE

(s, e) 

 $(a, b = a \odot s + e)$

$y_1,\ y_2$ small

$W = a \odot y_1 + y_2$

$c \hookleftarrow$ ChallengeSet

Our identification scheme based on MP-LWE

(s, e)

$(a, b = a \odot s + e)$

$y_1,\ y_2$ small

$W = a \odot y_1 + y_2$

$c \hookleftarrow$ ChallengeSet

$z_1 = c \odot s + y_1$

$z_2 = c \odot e + y_2$

reject z_1, z_2?

$Z = (z_1, z_2)$

Our identification scheme based on MP-LWE

(s, e)

$(a, b = a \odot s + e)$

$y_1,\ y_2$ small

$W = a \odot y_1 + y_2$

$c \hookleftarrow$ ChallengeSet

$z_1 = c \odot s + y_1$

$z_2 = c \odot e + y_2$

reject z_1, z_2?

$Z = (z_1, z_2)$

check if:

$W = a \odot z_1 + z_2 - c \odot b$

$z_1,\ z_2$ small

MPSign: from ID to DS using Fiat-Shamir

(s, e)  m  $(a, b = a \odot s + e)$

MPSign: from ID to DS using Fiat-Shamir

(s, e)  m

 $(a, b = a \odot s + e)$

$y_1,\ y_2$ small

$W = a \odot y_1 + y_2$

MPSign: from ID to DS using Fiat-Shamir

(s, e)  m

 $(a, b = a \odot s + e)$

$y_1,\ y_2$ small

$W = a \odot y_1 + y_2$

$c = H(W||m)$

MPSign: from ID to DS using Fiat-Shamir

(s, e)  m

 $(a, b = a \odot s + e)$

$y_1,\ y_2$ small

$W = a \odot y_1 + y_2$

$c = H(W||m)$

$z_1 = c \odot s + y_1$

$z_2 = c \odot e + y_2$

reject z_1, z_2?

MPSign: from ID to DS using Fiat-Shamir

(s, e)  m

 $(a, b = a \odot s + e)$

$y_1,\ y_2$ small

$W = a \odot y_1 + y_2$

$c = H(W||m)$

$z_1 = c \odot s + y_1$

$z_2 = c \odot e + y_2$

reject z_1, z_2?

MPSign: from ID to DS using Fiat-Shamir

(s, e)  m

 $(a, b = a \odot s + e)$

$y_1,\ y_2$ small

$W = a \odot y_1 + y_2$

$c = H(W||m)$

$(m, (z_1, z_2, c))$

$z_1 = c \odot s + y_1$

$z_2 = c \odot e + y_2$

reject z_1, z_2?

MPSign: from ID to DS using Fiat-Shamir

(s, e)  m

 $(a, b = a \odot s + e)$

$y_1,\ y_2$ small

$W = a \odot y_1 + y_2$

$c = H(W||m)$

$z_1 = c \odot s + y_1$

$z_2 = c \odot e + y_2$

reject z_1, z_2?

$(m, (z_1, z_2, c))$

$W = a \odot z_1 + z_2 - c \odot b$

MPSign: from ID to DS using Fiat-Shamir

(s, e)  m

 $(a, b = a \odot s + e)$

$y_1,\ y_2$ small

$W = a \odot y_1 + y_2$

$W = a \odot z_1 + z_2 - c \odot b$

$c = H(W||m)$

$(m, (z_1, z_2, c))$

$z_1 = c \odot s + y_1$

$z_2 = c \odot e + y_2$

reject z_1, z_2?

check if:

$c = H(W, m)$

$z_1,\ z_2$ small

Correctness and Security of MPSign

- correctness uses the associativity property of middle product

Correctness and Security of MPSign

- correctness uses the associativity property of middle product
- we fix the wrong security analysis from [Hir18]
  - they incorrectly assume $a \odot_n y$ is uniform for fixed y and uniform a

[KLS18]: ID has some "good properties" $\Rightarrow$ DS is tightly secure in QROM

Concrete parameters for MPSign

	$\lambda_Q = 143$	$\lambda_Q = 89$
degree of a	3800	2500
degree of z_2	1910	1300
degree of c	512	512
q	$\approx 2^{91}$	$\approx 2^{87}$
public key size	26.9 KB	19.5 KB
secret key size	1.1 KB	0.8 KB
signature size	20.1 KB	12.8 KB

- chosen accordingly to the best known attacks with the coreSVP hardness methodology

MPSign vs [Lyu16]

$\lambda = 89$	MPSign	[Lyu16]
public key size	19.5 KB	9.6 KB
secret key size	0.8 KB	8.8 KB
signature size	12.8 KB	27 KB

MPSign vs [Lyu16]

$\lambda = 89$	MPSign	[Lyu16]
public key size	19.5 KB	9.6 KB
secret key size	0.8 KB	8.8 KB
signature size	12.8 KB	27 KB

- our security proof is tight, while [Lyu16] is not
- we give an efficient key recovery attack on [Lyu16] when sk has very small coefficients

  $\Rightarrow$ you cannot decrease too much the size of the secret key in [Lyu16] to improve it

Summary

- we proved hardness of MP-LWE with short secrets
- we built a digital signature scheme whose security in QROM is based on it
- we provide concrete parameters for our scheme
- we provide a proof-of-concept implementation in Sage
  - https://github.com/pqc-ntrust/middle-product-LWE-signature