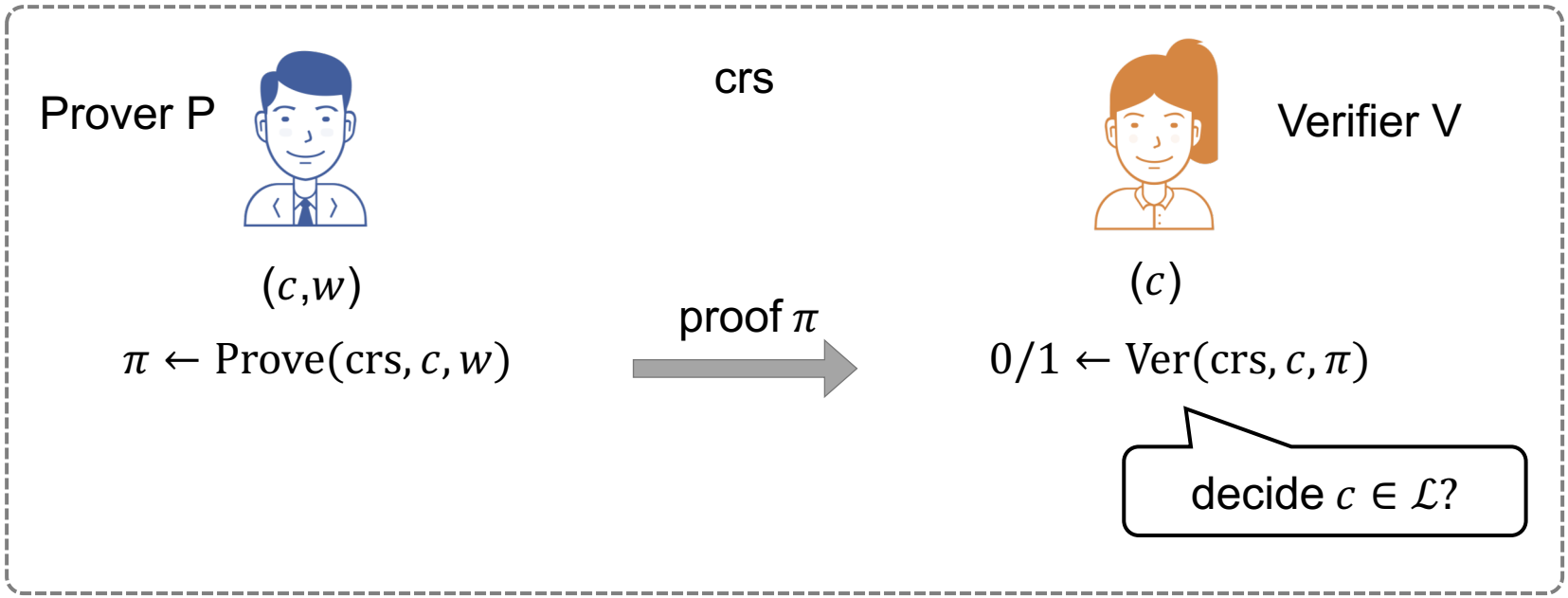
Fine-grained Verifier NIZK and Its Applications

Xiangyu Liu, Shengli Liu, Shuai Han, Dawu Gu
Shanghai Jiao Tong University
May 10, 2023

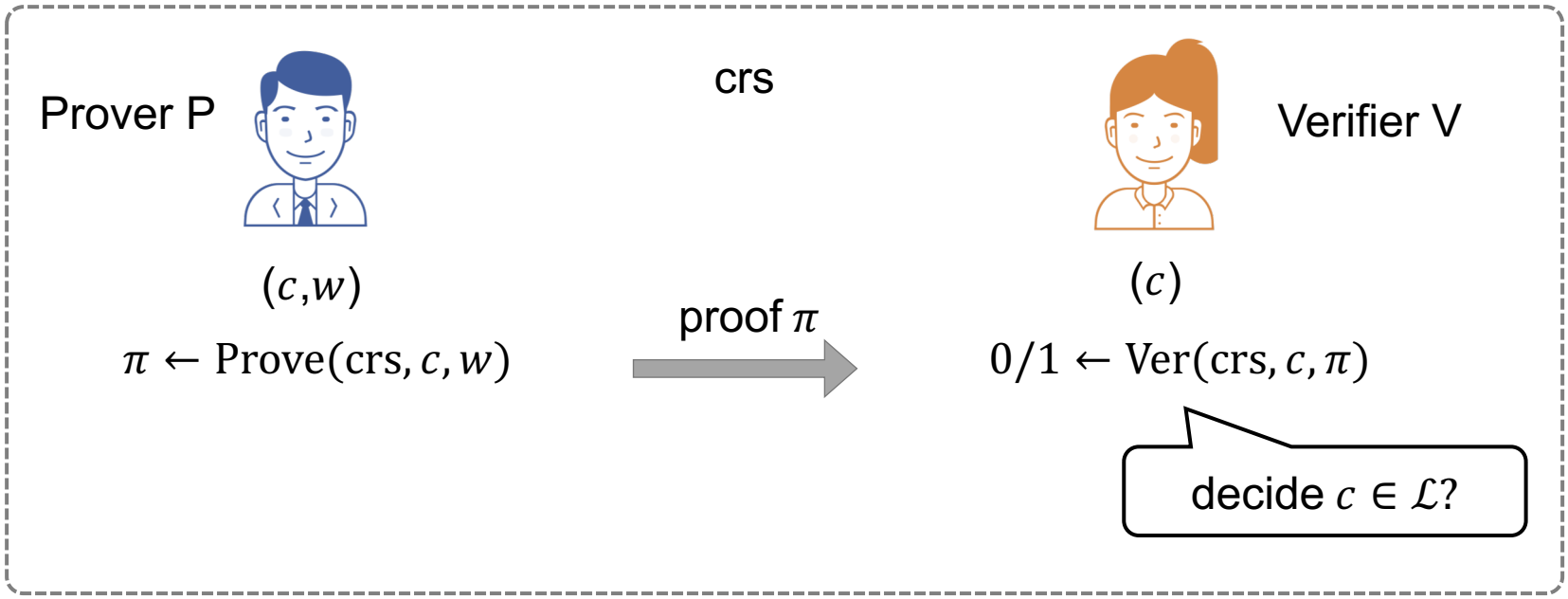
NIZK (Non-Interactive Zero-Knowledge)

- Language $\mathcal{L}$ defined by Relation R:
  instance $c \in \mathcal{L}$ iff exists a witness w s.t. $R(c, w) = 1$



QA-NIZK & DV-NIZK

- Language $\mathcal{L}$ defined by Relation R:
  instance $c \in \mathcal{L}$ iff exists a witness w s.t. $R(c, w) = 1$



- Quasi-Adaptive NIZK (QA-NIZK): crs depends on languages
- Designed-Verifier QA-NIZK (DV-NIZK): crs depends on languages, and Verification needs sk

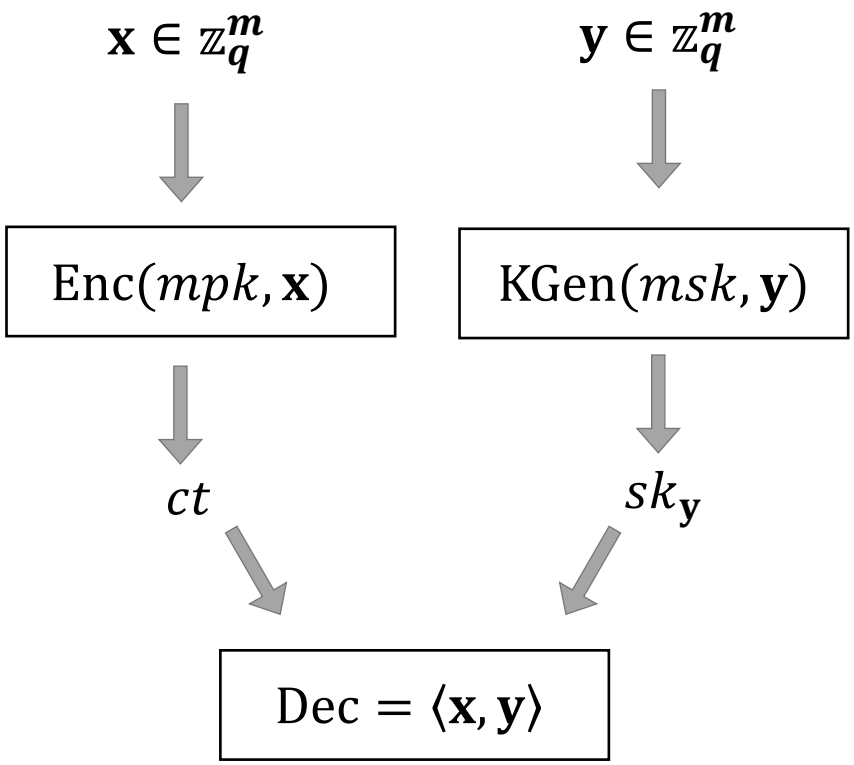
public verification

private verification
------ more succinct construction

Fine-grained verification setting: IPFE

IPFE: inner-product functional encryption

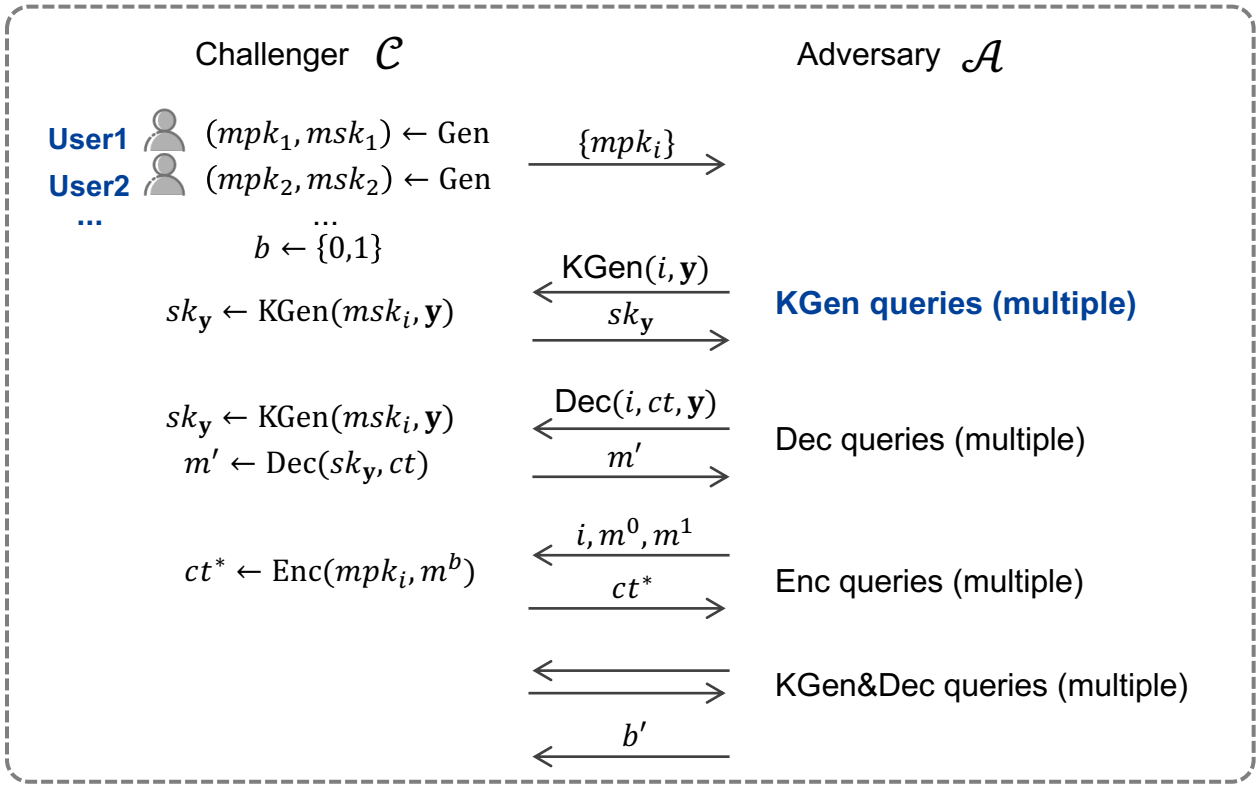
$$(mpk, msk) \leftarrow \mathrm{Gen}$$



Fine-grained verification setting: IPFE

Target: mCPA security to mCCA security

Idea: use NIZK, to prove the validity of ciphertexts

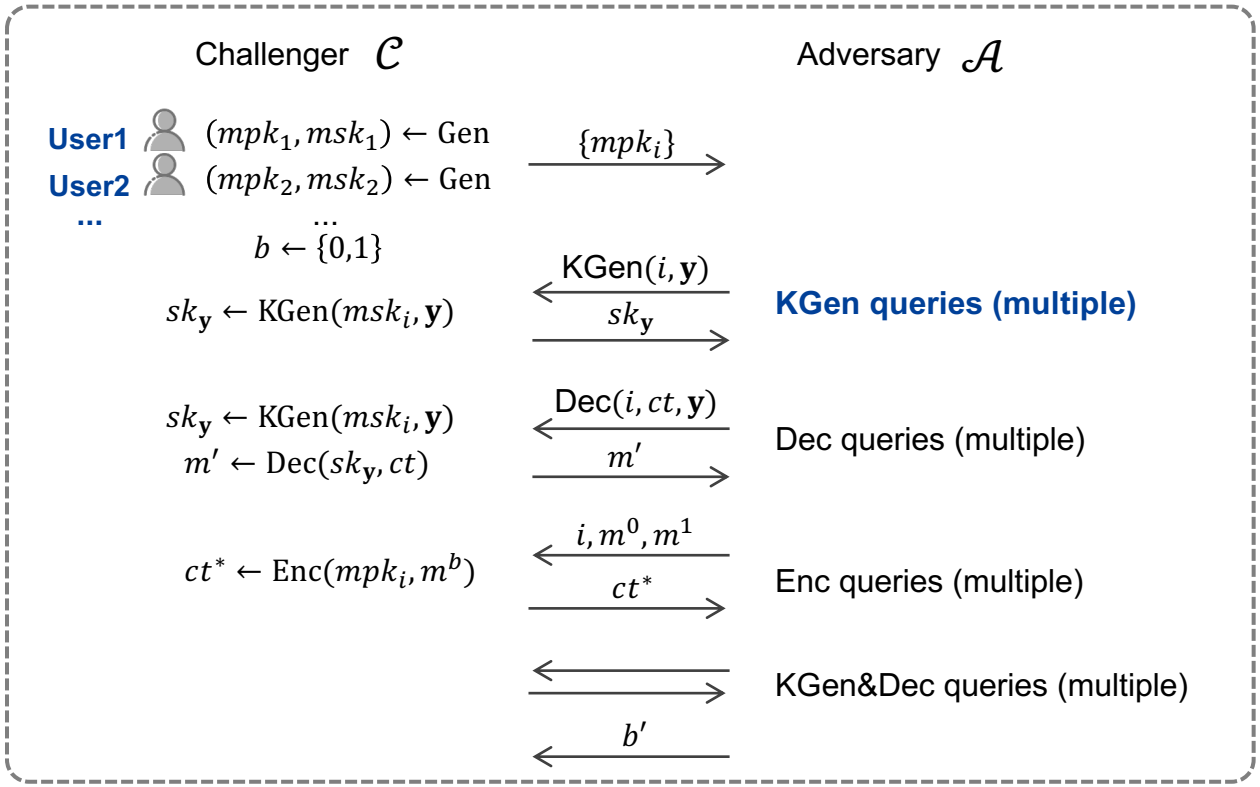


$\mathcal{A}$ obtains $sk_{\mathbf{y}}$ for $\mathbf{y}$

Fine-grained verification setting: IPFE

Target: mCPA security to mCCA security

Idea: use NIZK, to prove the validity of ciphertexts



$\mathcal{A}$ obtains $sk_{\mathbf{y}}$ for $\mathbf{y}$

- DV-NIZK (private verification): key derivation?
- QA-NIZK (public verification): overused?

Fine-grained verification setting: PKE

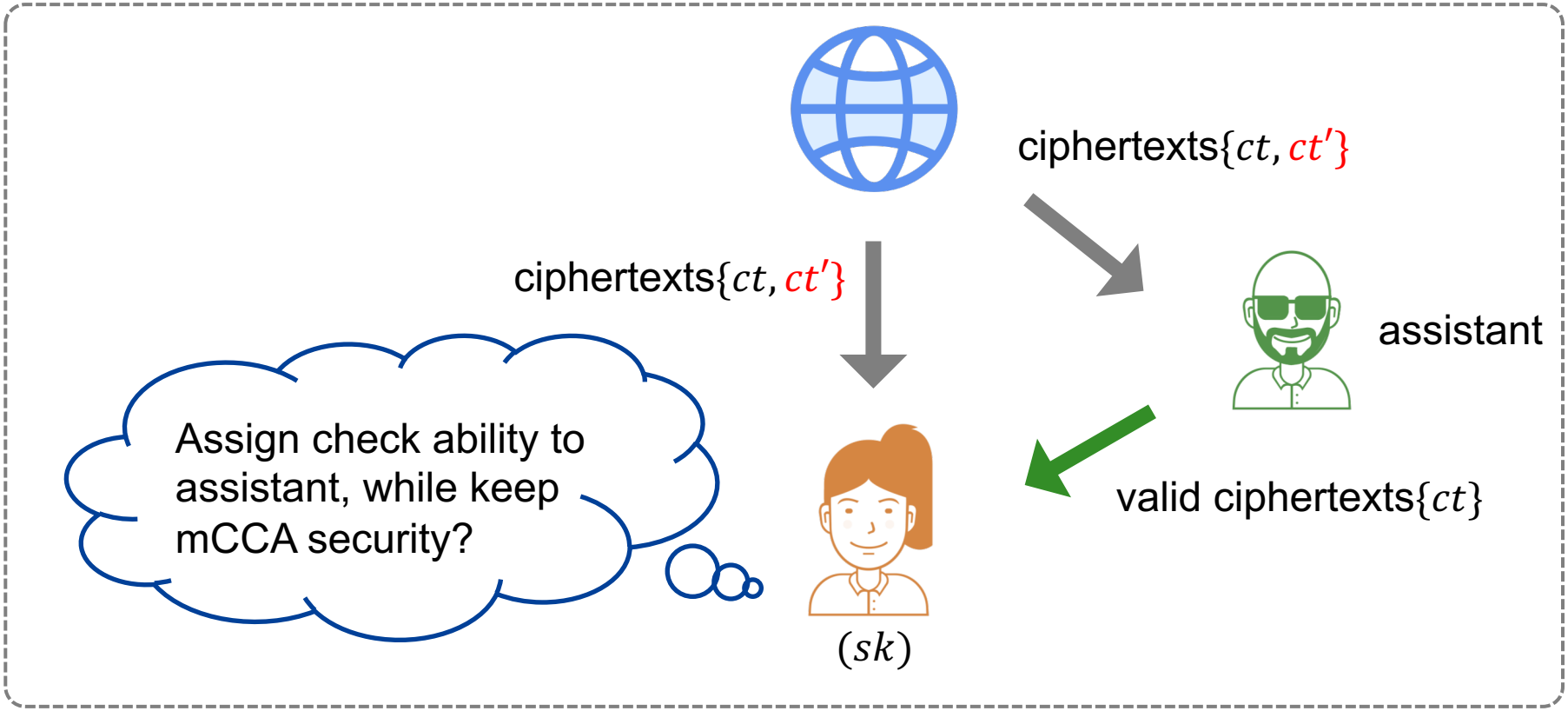
Target: designed ones can check the validities of ciphertexts (mCCA)

ciphertexts$\{ct, ct'\}$

(sk)

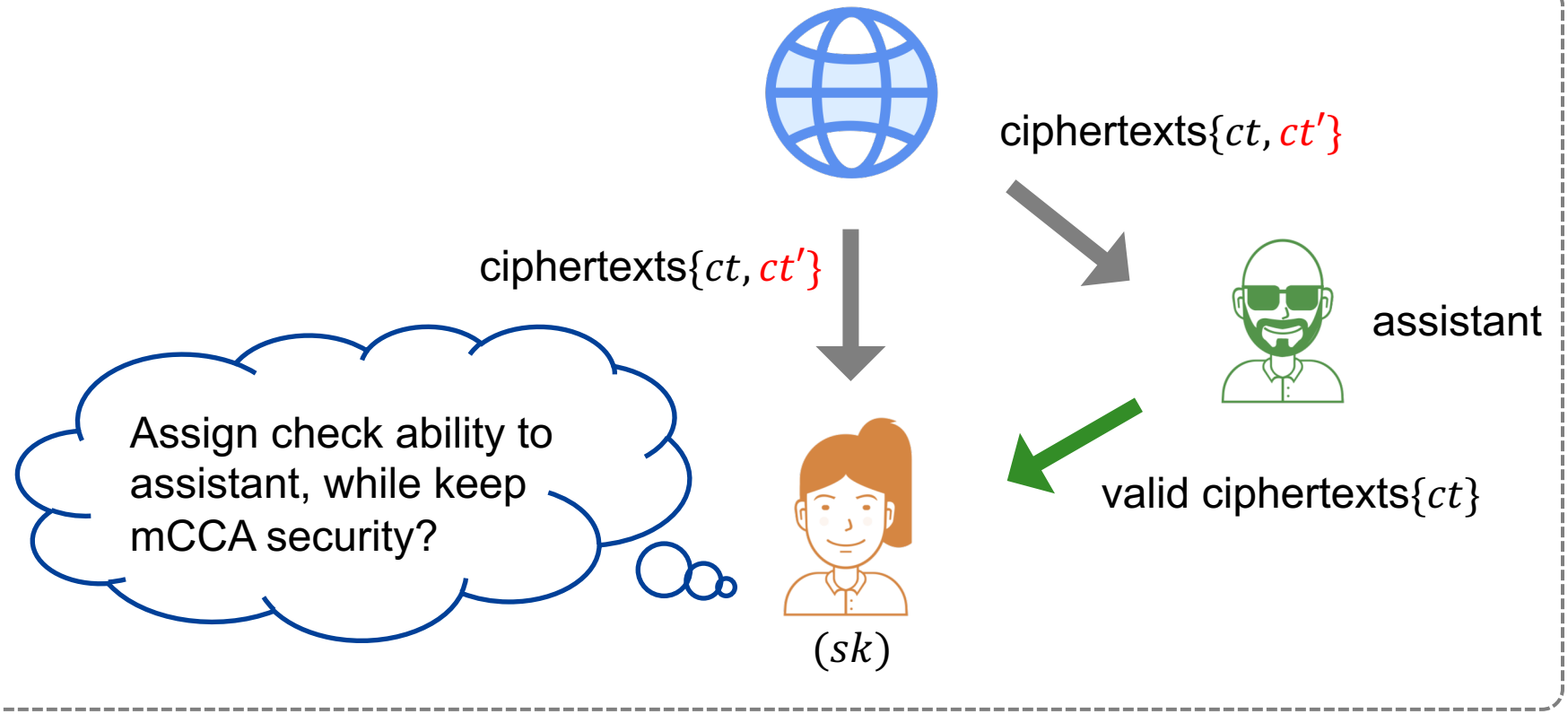
Fine-grained verification setting: PKE

Target: designed ones can check the validities of ciphertexts (mCCA)



Fine-grained verification setting: PKE

Target: designed ones can check the validities of ciphertexts (mCCA)



- DV-NIZK (private verification): no derivation?
- QA-NIZK (public verification): **no anonymity**?

Contributions:

- ✓ Fine-grained Verifier NIZK (FV-NIZK) :

  Two verification approaches:

  - $\mathrm{MVer}(msk, c, \pi)$ using msk
  - **Fine-grained Verify** $\mathrm{FVer}(sk_d, c, \pi)$ using derived key sk_d , $d \in \mathcal{D}$

  Security:

  - **verification soundness, unbounded simulation soundness (USS), proof pseudorandomness**

- ✓ Two constructions for **linear subspace language** with tight security
  - pairing-free, $L = O(\lambda)$
  - pairing-based, $L = O(\log \lambda)$

- ✓ Applications
  - mCCA-secure IPFE
  - Fine-grained Verifiable PKE (FV-PKE)

Start point: DV-NIZK

(tag-based) DV-NIZK in [GHKW16] (to prove $[\mathbf{c}] = [\mathbf{A}]\mathbf{s} \in \mathrm{Span}([\mathbf{A}])$):

$$\begin{cases} msk = \left(\mathbf{k}, \{\widehat{\boldsymbol{k}}_{\ell,b}^T\}_{\ell,b}\right) \\ crs = \left([\mathbf{A}], [\mathbf{k}^T\mathbf{A}], [\mathbf{B}], \left\{\left[\widehat{\boldsymbol{k}}_{\ell,b}^T\mathbf{B}\right]\right\}_{\ell,b}\right) \\ \tau \in \{0,1\}^\lambda \end{cases} \qquad \pi = \begin{cases} [\mathbf{t}] = [\mathbf{B}]\mathbf{r} \\ [u] \end{cases}$$

$$u = \mathbf{k}^T \mathbf{A}\, \mathbf{s} + \widehat{\boldsymbol{k}}_\tau^T \mathbf{B}\, \mathbf{r} \qquad \widehat{\boldsymbol{k}}_\tau := \sum_{\ell=1}^{\lambda} \widehat{\boldsymbol{k}}_{\ell,\tau_\ell}$$

Prove: $[u] = [\mathbf{k}^T \cdot \mathbf{A}] \cdot \mathbf{s} + \left[\widehat{\boldsymbol{k}}_\tau^T \cdot \mathbf{B}\right] \cdot \mathbf{r}$

Ver: $[u] \stackrel{?}{=} \mathbf{k}^T \cdot [\mathbf{c}] + \widehat{\boldsymbol{k}}_\tau^T \cdot [\mathbf{t}]$

Linearity!

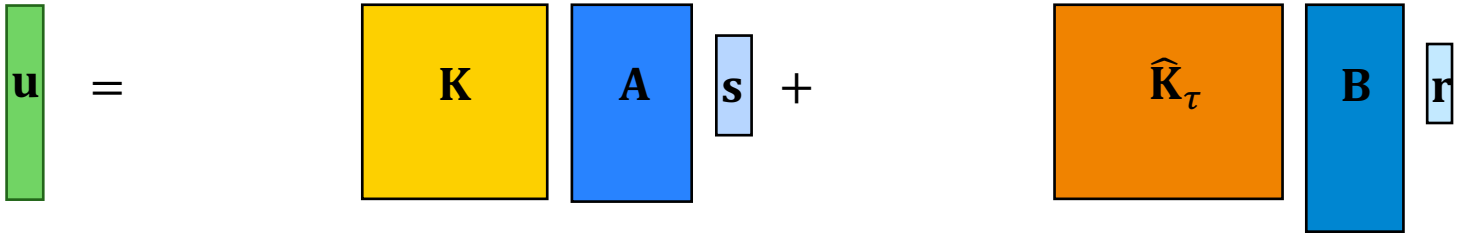
[GHKW16] Gay, R., Hofheinz, D., Kiltz, E., Wee, H.: Tightly cca-secure encryption without pairings.

Idea 1: extend msk to matrices

Let $\mathbf{d} \in \mathbb{Z}_q^m$, FV-NIZK attempt 1 (to prove $[\mathbf{c}] = [\mathbf{A}]\mathbf{s} \in \mathrm{Span}([\mathbf{A}])$):

$$\begin{cases} msk = \left(\mathbf{K}, \{\widehat{\mathbf{K}}_{\ell,b}\}_{\ell,b}\right) \\ crs = \left([\mathbf{A}], [\mathbf{KA}], [\mathbf{B}], \left\{\left[\widehat{\mathbf{K}}_{\ell,b}\mathbf{B}\right]\right\}_{\ell,b}\right) \\ \tau \in \{0,1\}^\lambda \end{cases} \qquad \pi = \begin{cases} [\mathbf{t}] = [\mathbf{B}]\mathbf{r} \\ [\mathbf{u}] \end{cases}$$

$$\widehat{\mathbf{K}}_\tau := \sum_{\ell=1}^{\lambda} \widehat{\mathbf{K}}_{\ell,\tau_\ell}$$



Prove: $[\mathbf{u}] = [\mathbf{K} \cdot \mathbf{A}] \cdot \mathbf{s} + \left[\widehat{\mathbf{K}}_\tau \cdot \mathbf{B}\right] \cdot \mathbf{r}$

MVer: $[\mathbf{u}] \stackrel{?}{=} \mathbf{K} \cdot [\mathbf{c}] + \widehat{\mathbf{K}}_\tau \cdot [\mathbf{t}]$

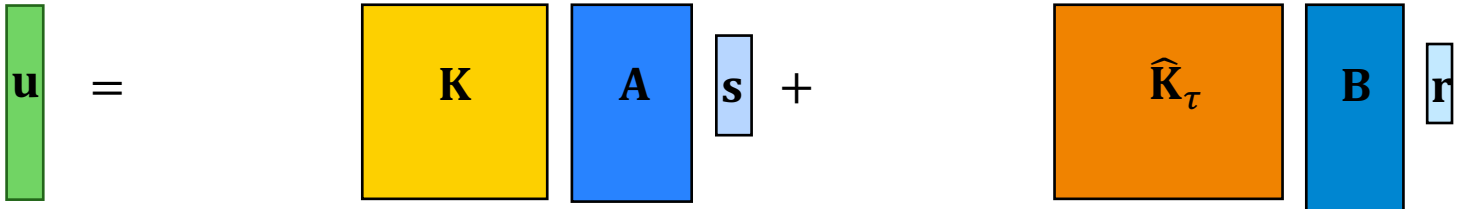
Idea 1: extend msk to matrices

Let $\mathbf{d} \in \mathbb{Z}_q^m$, FV-NIZK attempt 1 (to prove $[\mathbf{c}] = [\mathbf{A}]\mathbf{s} \in \mathrm{Span}([\mathbf{A}])$):

$$\begin{cases} msk = \left(\mathbf{K}, \{\widehat{\mathbf{K}}_{\ell,b}\}_{\ell,b}\right) \\ crs = \left([\mathbf{A}], [\mathbf{KA}], [\mathbf{B}], \left\{\left[\widehat{\mathbf{K}}_{\ell,b}\mathbf{B}\right]\right\}_{\ell,b}\right) \\ \tau \in \{0,1\}^\lambda \end{cases} \qquad \pi = \begin{cases} [\mathbf{t}] = [\mathbf{B}]\mathbf{r} \\ [\mathbf{u}] \end{cases}$$

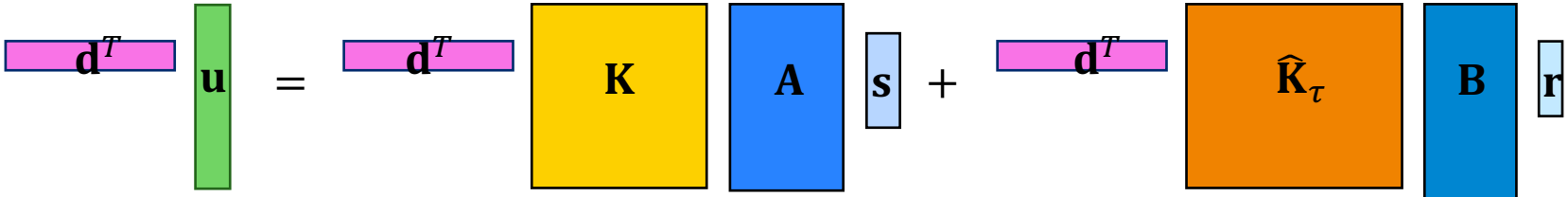
$$\widehat{\mathbf{K}}_\tau := \sum_{\ell=1}^{\lambda} \widehat{\mathbf{K}}_{\ell,\tau_\ell}$$

$$sk_{\mathbf{d}} = \left(\mathbf{d}^T, \mathbf{d}^T\mathbf{K}, \{\mathbf{d}^T\widehat{\mathbf{K}}_{\ell,b}\}_{\ell,b}\right)$$



Prove: $[\mathbf{u}] = [\mathbf{K} \cdot \mathbf{A}] \cdot \mathbf{s} + \left[\widehat{\mathbf{K}}_\tau \cdot \mathbf{B}\right] \cdot \mathbf{r}$

MVer: $[\mathbf{u}] \stackrel{?}{=} \mathbf{K} \cdot [\mathbf{c}] + \widehat{\mathbf{K}}_\tau \cdot [\mathbf{t}]$



FVer: $\mathbf{d}^T \cdot [\mathbf{u}] \stackrel{?}{=} \mathbf{d}^T \cdot \mathbf{K} \cdot [\mathbf{c}] + \mathbf{d}^T \cdot \widehat{\mathbf{K}}_\tau \cdot [\mathbf{t}]$

Idea 1: extend msk to matrices

Let $\mathbf{d} \in \mathbb{Z}_q^m$, FV-NIZK attempt 1 (to prove $[\mathbf{c}] = [\mathbf{A}]\mathbf{s} \in \mathrm{Span}([\mathbf{A}])$):

msk

crs

$\tau \in$

$\tau := \sum_{\ell=1}^{\lambda} \widehat{\mathbf{K}}_{\ell,\tau_\ell}$

Two **problems** :

1. MVer and FVer are not statistically equivalent
2. msk is fully exposed after m times key derivation for linear independent $\mathbf{d}$

Prove: $[\mathbf{u}] = [\mathbf{K} \cdot \mathbf{A}] \cdot \mathbf{s} + [\widehat{\mathbf{K}}_\tau \cdot \mathbf{B}] \cdot \mathbf{r}$

MVer: $[\mathbf{u}] \stackrel{?}{=} \mathbf{K} \cdot [\mathbf{c}] + \widehat{\mathbf{K}}_\tau \cdot [\mathbf{t}]$

$\mathbf{d}^T \mathbf{u} = \mathbf{d}^T \mathbf{K} \mathbf{A} \mathbf{s} + \mathbf{d}^T \widehat{\mathbf{K}}_\tau \mathbf{B} \mathbf{r}$

FVer: $\mathbf{d}^T \cdot [\mathbf{u}] \stackrel{?}{=} \mathbf{d}^T \cdot \mathbf{K} \cdot [\mathbf{c}] + \mathbf{d}^T \cdot \widehat{\mathbf{K}}_\tau \cdot [\mathbf{t}]$

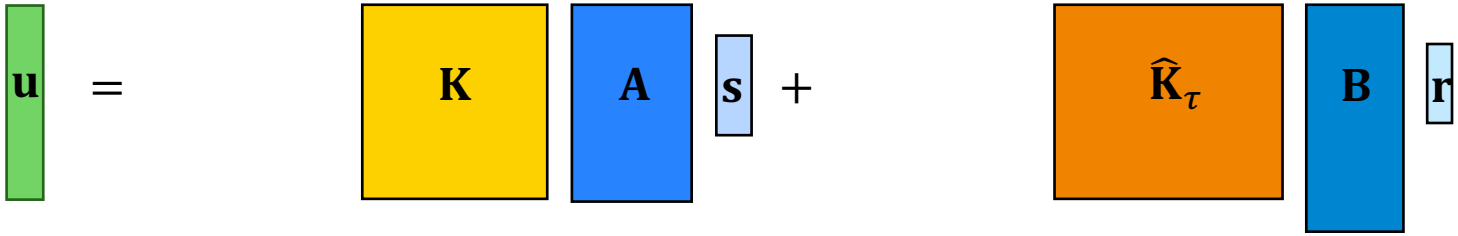
Step 2: introduce a random matrix M

Let $\mathbf{d} \in \mathbb{Z}_q^m$, FV-NIZK attempt 1 (to prove $[\mathbf{c}] = [\mathbf{A}]\mathbf{s} \in \mathrm{Span}([\mathbf{A}])$):

$$\begin{cases} msk = \left(\mathbf{M} \in \mathbb{Z}_q^{m\times(m+1)}, \mathbf{K}, \{\widehat{\mathbf{K}}_{\ell,b}\}_{\ell,b}\right) \\ crs = \left([\mathbf{A}], [\mathbf{KA}], [\mathbf{B}], \{[\widehat{\mathbf{K}}_{\ell,b}\mathbf{B}]\}_{\ell,b}\right) \\ \tau \in \{0,1\}^\lambda \end{cases} \qquad \pi = \begin{cases} [\mathbf{t}] = [\mathbf{B}]\mathbf{r} \\ [\mathbf{u}] \end{cases}$$

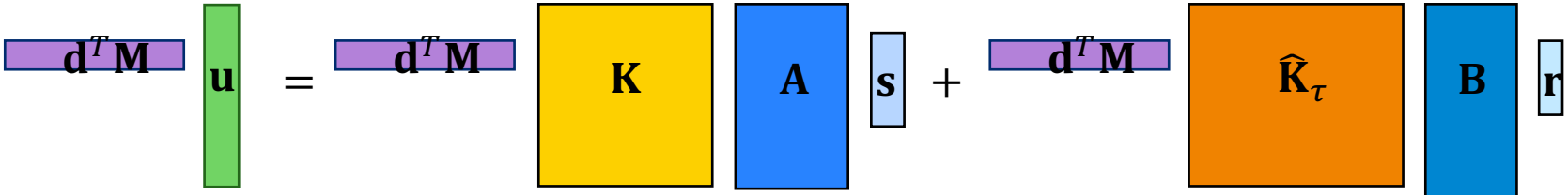
$$\widehat{\mathbf{K}}_\tau := \sum_{\ell=1}^{\lambda} \widehat{\mathbf{K}}_{\ell,\tau_\ell}$$

$$sk_{\mathbf{d}} = \left(\mathbf{d}^T\mathbf{M}, \mathbf{d}^T\mathbf{M}\mathbf{K}, \{\mathbf{d}^T\mathbf{M}\widehat{\mathbf{K}}_{\ell,b}\}_{\ell,b}\right)$$



Prove: $[\mathbf{u}] = [\mathbf{K} \cdot \mathbf{A}] \cdot \mathbf{s} + \left[\widehat{\mathbf{K}}_\tau \cdot \mathbf{B}\right] \cdot \mathbf{r}$

MVer: $[\mathbf{u}] \stackrel{?}{=} \mathbf{K} \cdot [\mathbf{c}] + \widehat{\mathbf{K}}_\tau \cdot [\mathbf{t}]$



FVer: $\mathbf{d}^T\mathbf{M} \cdot [\mathbf{u}] \stackrel{?}{=} \mathbf{d}^T\mathbf{M} \cdot \mathbf{K} \cdot [\mathbf{c}] + \mathbf{d}^T\mathbf{M} \cdot \widehat{\mathbf{K}}_\tau \cdot [\mathbf{t}]$

Step 2: introduce a random matrix M

Let $\mathbf{d} \in \mathbb{Z}_q^m$, FV-NIZK attempt 1 (to prove $[\mathbf{c}] = [\mathbf{A}]\mathbf{s} \in \mathrm{Span}([\mathbf{A}])$):

msk

crs

$\tau \in$

$\widehat{\mathbf{K}}_{\ell,\tau_\ell}$

Solve the two **problems** :

1. MVer and FVer are not statistically equivalent?

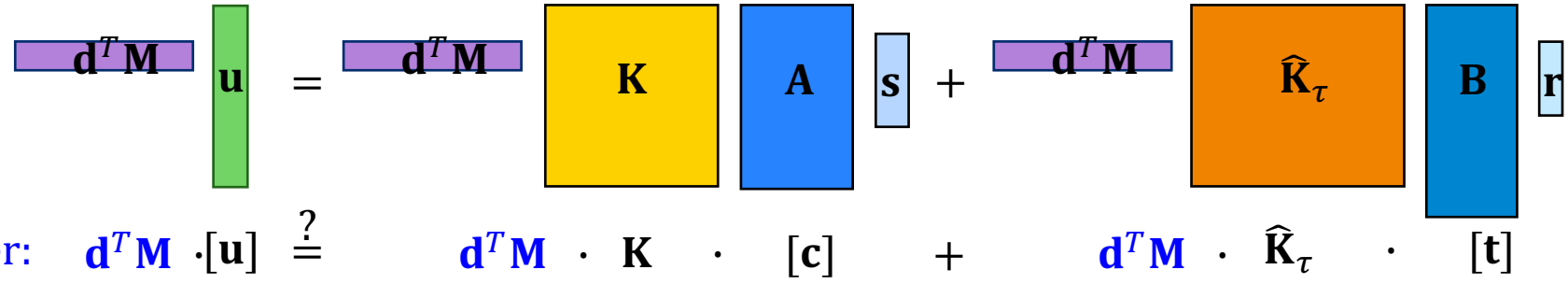
------ $\mathbf{d}^T\mathbf{M}$ distributs uniformly over $\mathbb{Z}_q^{\mathbf{1}\times(\boldsymbol{m}+\mathbf{1})}$ to Adversary

2. msk is fully exposed after m times key derivation for linear independent $\mathbf{d}$

------ since $\mathbf{M} \in \mathbb{Z}_q^{\boldsymbol{m}\times(\boldsymbol{m}+\mathbf{1})}$, some entropy is left in msk

Prove:

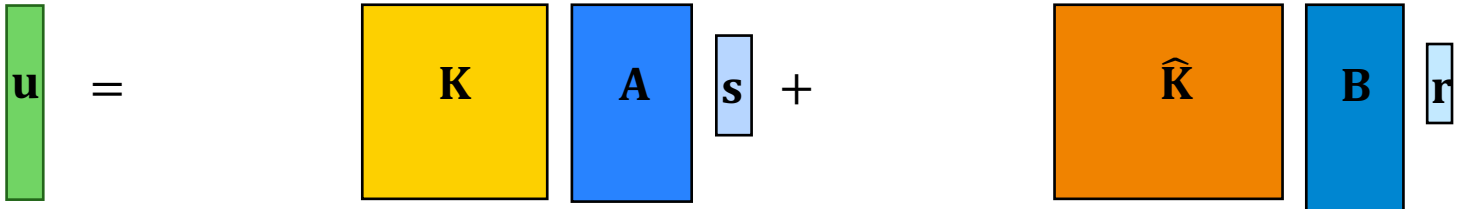
MVer:



FV-NIZK construction 2

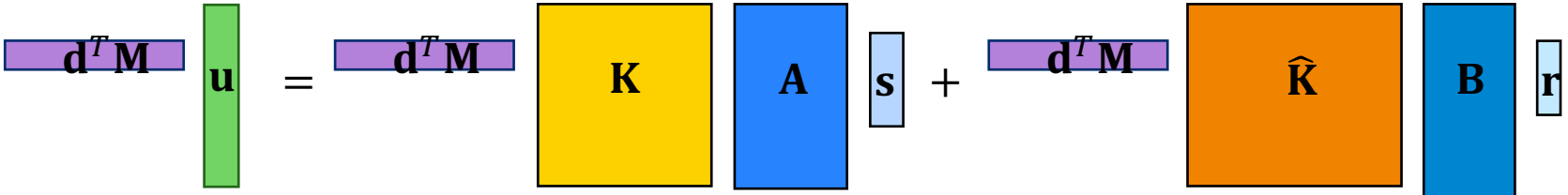
Let $\mathbf{d} \in \mathbb{Z}_q^m$, FV-NIZK attempt 2 (to prove $[\mathbf{c}] = [\mathbf{A}]\mathbf{s} \in \mathrm{Span}([\mathbf{A}])$):

$$\begin{cases} msk = \left(\mathbf{M} \in \mathbb{Z}_q^{m\times(m+1)}, \mathbf{K}, \widehat{\mathbf{K}}\right) \\ crs = \left([\mathbf{A}], [\mathbf{KA}], [\mathbf{B}_0], [\widehat{\mathbf{K}}\mathbf{B}_0]\right) \\ \tau \in \{0,1\}^\lambda \end{cases} \quad \pi = \begin{cases} [\mathbf{t}] = [\mathbf{B}_0]\mathbf{r} \\ [\mathbf{u}] \\ \pi_{or} \end{cases} \quad sk_{\mathbf{d}} = \left(\mathbf{d}^T\mathbf{M}, \mathbf{d}^T\mathbf{MK}, \mathbf{d}^T\mathbf{M}\widehat{\mathbf{K}}\right)$$



Prove: $[\mathbf{u}] = [\mathbf{K} \cdot \mathbf{A}] \cdot \mathbf{s} + \left[\widehat{\mathbf{K}} \cdot \mathbf{B}\right] \cdot \mathbf{r}$

MVer: $[\mathbf{u}] \stackrel{?}{=} \mathbf{K} \cdot [\mathbf{c}] + \widehat{\mathbf{K}} \cdot [\mathbf{t}]$



FVer: $\mathbf{d}^T\mathbf{M} \cdot [\mathbf{u}] \stackrel{?}{=} \mathbf{d}^T\mathbf{M} \cdot \mathbf{K} \cdot [\mathbf{c}] + \mathbf{d}^T\mathbf{M} \cdot \widehat{\mathbf{K}} \cdot [\mathbf{t}]$

[AJO+19] Abe, M., Jutla, C.S., Ohkubo, M., Pan, J., Roy, A., Wang, Y.: Shorter QA-NIZK and SPS with tighter security.

Application: mCCA IPFE

- IPFE from mCPA to mCCA

$$msk = (\widetilde{\text{IPFE}}.msk, \Pi.msk)$$

$\text{Enc}(mpk, \mathbf{x})$:

$s \leftarrow \mathbb{Z}_q^m$

ct {
- $[\mathbf{c}] := [\mathbf{As}]$
- $[\boldsymbol{d}] := [\mathbf{WAs} + \mathbf{x}]$
- $\pi \leftarrow \Pi.\text{Prove}([\mathbf{c}], \mathbf{s}, \tau)$

$\text{KGen}(msk, \mathbf{y})$:

$sk_{\mathbf{y}}$ {
- $-\mathbf{y}^T\mathbf{W}$
- $\mathbf{y}^T$
- $\Pi.sk_{\mathbf{y}} \leftarrow \Pi.\text{Delegate}(\Pi.msk, \mathbf{y})$

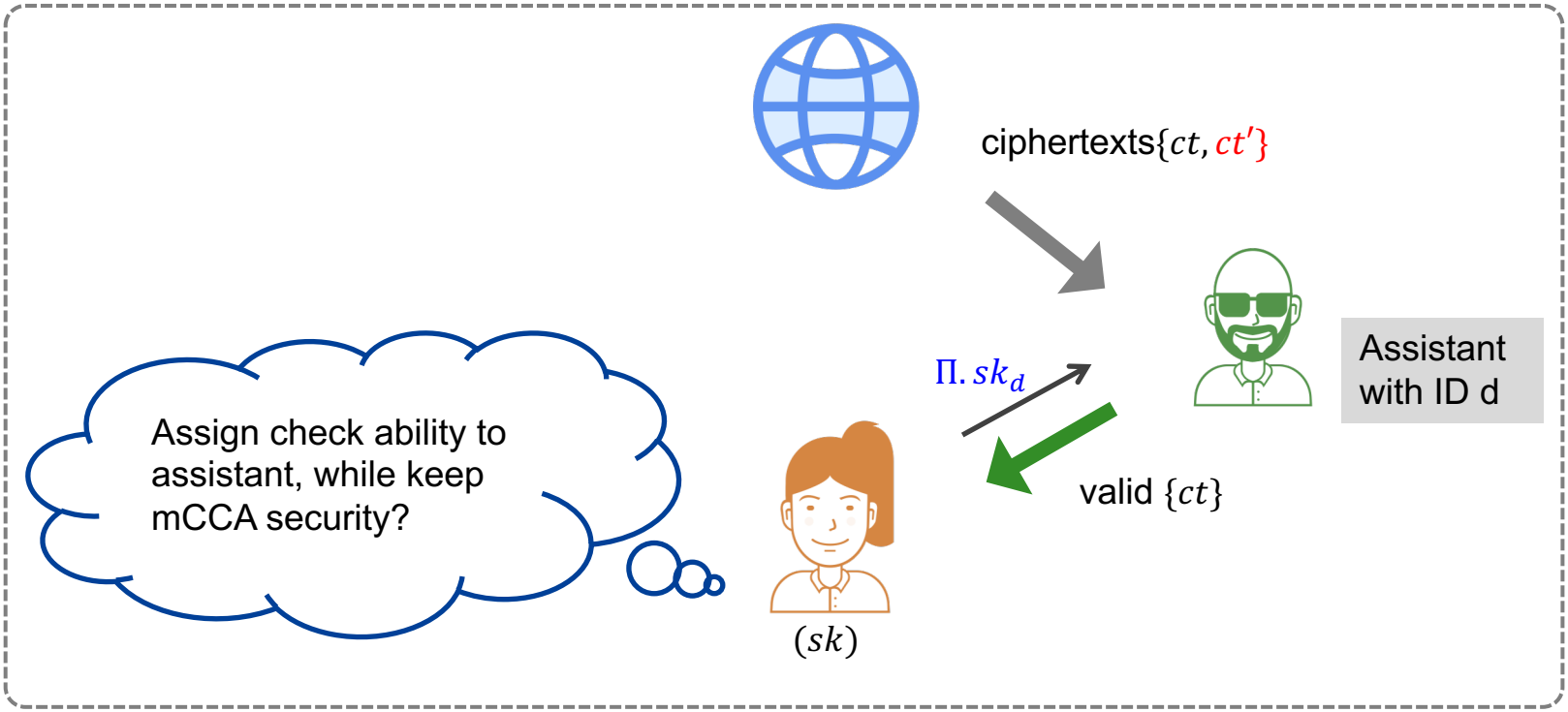
- $\tau = H([\mathbf{c}], [\mathbf{d}])$
- π is an FV-NIZK proof for $[\mathbf{c}] \in \text{Span}([\mathbf{A}])$

✓ FV-NIZK Π support key derivation ➔ IPFE setting

✓ USS holds after deriving $\Pi.sk_d$ ➔ mCCA security

Application: fine-grained verifiable PKE

- Fine-grained Verifiable PKE (FV-PKE):



- ✓ FV-NIZK Π support key derivation ➔ derive key to check validity
- ✓ USS holds after deriving $\Pi.sk_d$ ➔ mCCA security

Conclusion

- ✓ Fine-grained Verifier NIZK (FV-NIZK), supports fine-grained verification algorithms
- ✓ Two constructions for **linear subspace language** with tight security
- ✓ Applications in IPFE and FV-PKE

Conclusion

- ✓ Fine-grained Verifier NIZK (FV-NIZK), supports fine-grained verification algorithms
- ✓ Two constructions for **linear subspace language** with tight security
- ✓ Applications in IPFE and FV-PKE

Thank you!

Xiangyu Liu (xiangyu1994liu@gmail.com)