RSAConference2019
San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: CRYP-F02

Revisiting the Secret Hiding Assumption Used in Verifiable (Outsourced) Computation

Liang Zhao

Assistant Professor
Sichuan University, China

四川大學
SICHUAN UNIVERSITY

Agenda of My Presentation

① Background Information

② Attack Strategy

③ Analysis for the Decisional Secret Hiding Assumption

④ Privacy Analysis for Atallah-Frikken Protocols

⑤ Experimental Verification

Outline

① Background Information

② Attack Strategy

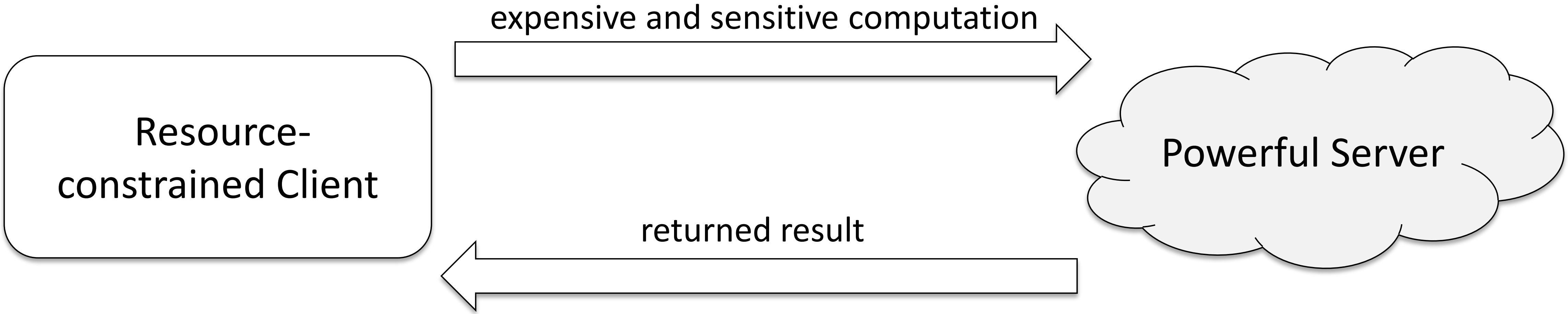
③ Analysis for the Decisional Secret Hiding Assumption

④ Privacy Analysis for Atallah-Frikken Protocols

⑤ Experimental Verification

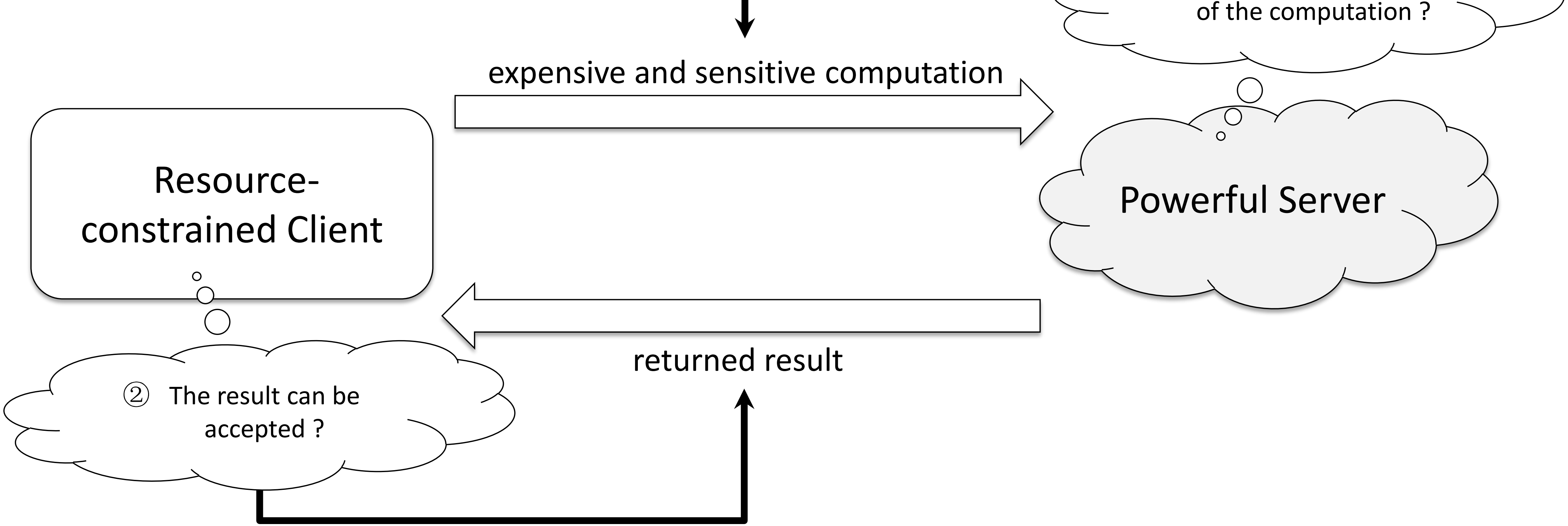
Background Information

- The general scenario about the reasonable outsourcing computation:



Background Information

The considered Privacy-preserving Verifiable (outsourced) Computation (PVC):



Background Information

- Atallah and Frikken proposed a new hardness assumption called the Secret Hiding assumption (SH) at ACM AsiaCCS 2010 [Atallah & Frikken'10]

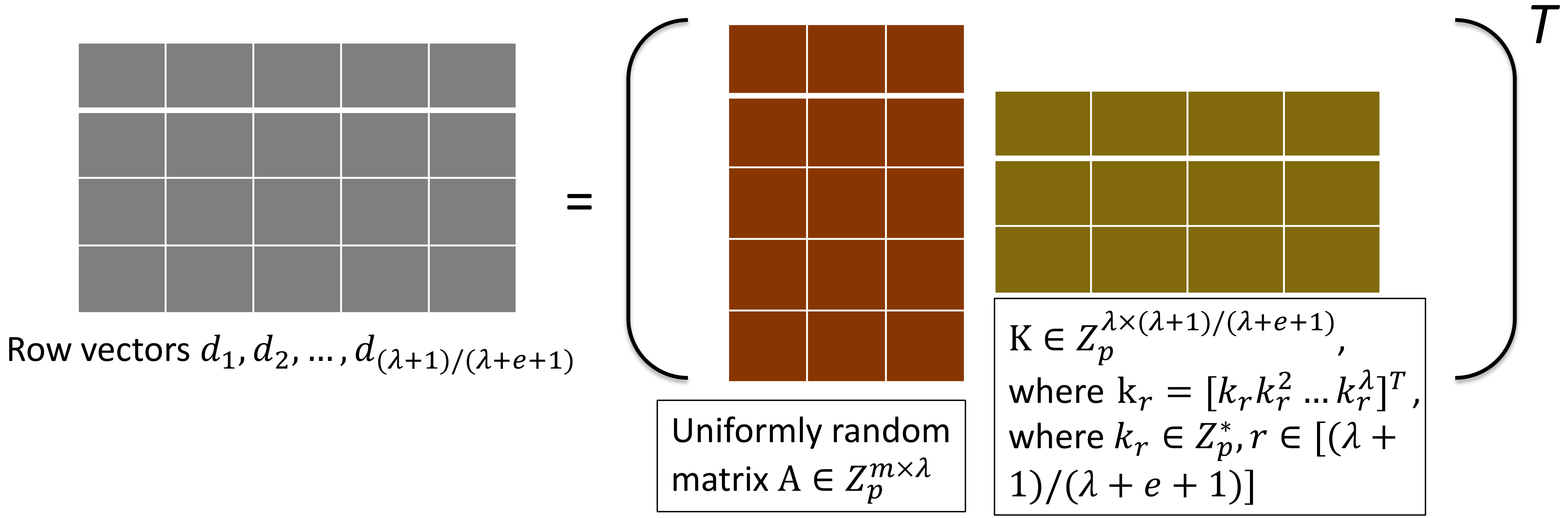
- Two concrete versions:
  - ✓ Weak SH assumption (WSH)
  - ✓ Strong SH assumption (SSH)

Background Information

- What is the WSH/SSH assumption ?

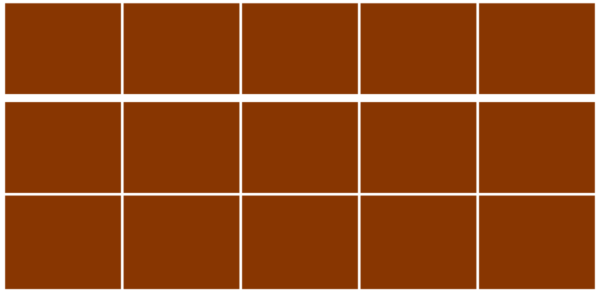
What is the WSH/SSH distribution ?

1



Background Information

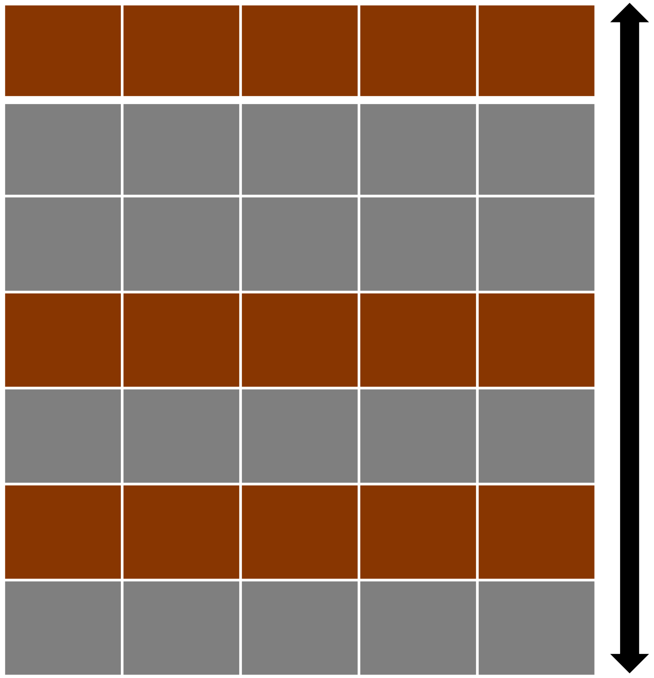
2



Choose some row vectors $u_1, u_2, \dots, u_{\lambda/(\lambda+e+1)}$ uniformly at random, where $u_r \in Z_p^m$

3

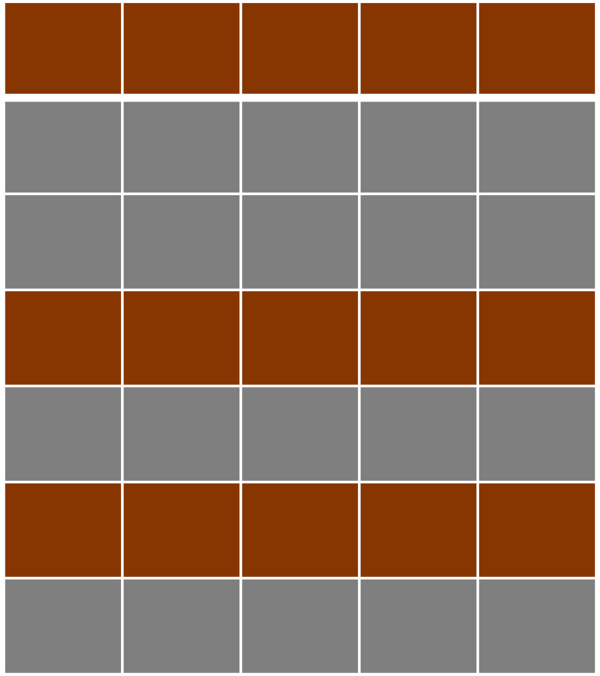
R =



Combine $d_1, d_2, \dots, d_{(\lambda+1)/(\lambda+e+1)}$ with $u_1, u_2, \dots, u_{\lambda/(\lambda+e+1)}$ to generate an $n \times m$ matrix R, and permute the rows of R, where $n \in \{2\lambda + 1, 2\lambda + 2e + 2\}$

Background Information

R =



Decision: Does R look random ?

Search: given R, find $k_1, k_2, \ldots, k_{(\lambda+1)/(\lambda+e+1)}$ or A

NOTE:

① The decisional-WSH is the same as the decisional-SSH

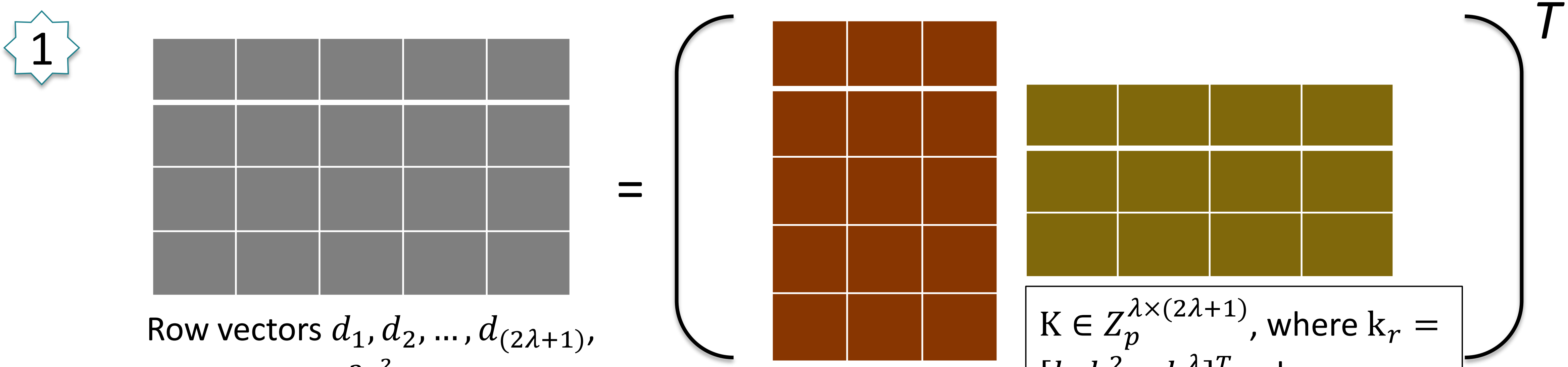
② The search-WSH is to find $k_1, k_2, \ldots, k_{(\lambda+1)}$ or A. The search-SSH is to find $k_1, k_2, \ldots, k_{(\lambda+e+1)}$ or A

WSH/SSH Assumption:

No polynomial-time adversary can solve the decisional and search WSH/SSH problem

Background Information

- Atallah and Frikken proposed some WSH/SSH-based PVC protocols for matrix multiplication
- The idea of the PVC protocols:



Row vectors $d_1, d_2, \ldots, d_{(2\lambda+1)}$, where $d_r \in Z_p^{2v^2}$

Uniformly random matrix $\mathrm{A} \in Z_p^{2v^2 \times \lambda}$

$\mathrm{K} \in Z_p^{\lambda \times (2\lambda+1)}$, where $\mathrm{k}_r = [k_r k_r^2 \ldots k_r^\lambda]^T$, where $k_r \in Z_p^*, r \in [2\lambda+1]$

Background Information

2 For two $v \times v$ matrices M_1 and M_2, use each vector d_r to mask them, and generate $2\lambda + 1$ matrix pairs $(\mathrm{C}_1(k_1), \mathrm{C}_2(k_1)), (\mathrm{C}_1(k_2), \mathrm{C}_2(k_2)), \ldots (\mathrm{C}_1(k_{2\lambda+1}), \mathrm{C}_2(k_{2\lambda+1}))$

$$\mathrm{C}_1(k_r)||\mathrm{C}_2(k_r) = d_r + \mathrm{M}_1||\mathrm{M}_2$$

3 *The Two-Server Case:* Choose 2λ $v \times v$ uniformly random matrices $\mathrm{B}_1, \mathrm{B}_2, \ldots, \mathrm{B}_{2\lambda}$ to create λ pairs $(\mathrm{B}_1, \mathrm{B}_2), \ldots, (\mathrm{B}_{2\lambda-1}, \mathrm{B}_{2\lambda})$. Send λ pairs $(\mathrm{C}_1(k_1), \mathrm{C}_2(k_1)), (\mathrm{C}_1(k_2), \mathrm{C}_2(k_2)), \ldots (\mathrm{C}_1(k_\lambda), \mathrm{C}_2(k_\lambda))$ to the first server. Combine $(\mathrm{B}_1, \mathrm{B}_2), \ldots, (\mathrm{B}_{2\lambda-1}, \mathrm{B}_{2\lambda})$ with $(\mathrm{C}_1(k_{\lambda+1}), \mathrm{C}_2(k_{\lambda+1})), \ldots, (\mathrm{C}_1(k_{2\lambda+1}), \mathrm{C}_2(k_{2\lambda+1}))$ to generate $2\lambda + 1$ matrix pairs and permute these matrix pairs. Send the $2\lambda + 1$ permuted matrix pairs to the second server

The Single-Server Case: Choose $(4\lambda + 2)$ $v \times v$ uniformly random matrices $\mathrm{B}_1, \mathrm{B}_2, \ldots, \mathrm{B}_{4\lambda+2}$ to create $2\lambda + 1$ pairs $(\mathrm{B}_1, \mathrm{B}_2), \ldots, (\mathrm{B}_{4\lambda+1}, \mathrm{B}_{4\lambda+2})$. Combine $(\mathrm{B}_1, \mathrm{B}_2), \ldots, (\mathrm{B}_{4\lambda+1}, \mathrm{B}_{4\lambda+2})$ with $(\mathrm{C}_1(k_1), \mathrm{C}_2(k_1)), \ldots (\mathrm{C}_1(k_{2\lambda+1}), \mathrm{C}_2(k_{2\lambda+1}))$ to generate $4\lambda + 2$ matrix pairs and permute these matrix pairs. Send the $4\lambda + 2$ permuted matrix pairs to a server

Background Information

4 *The Two-Server Case:* Send back the products of all matrix pairs computed by the two servers. Choose some products corresponding to M_1 and M_2, and interpolate these products to find the real result of $\mathrm{M}_1\mathrm{M}_2$

The Single-Server Case: Send back the products of all matrix pairs computed by a server. Choose some products corresponding to M_1 and M_2, and interpolate these products to find the real result of $\mathrm{M}_1\mathrm{M}_2$

Theorems:

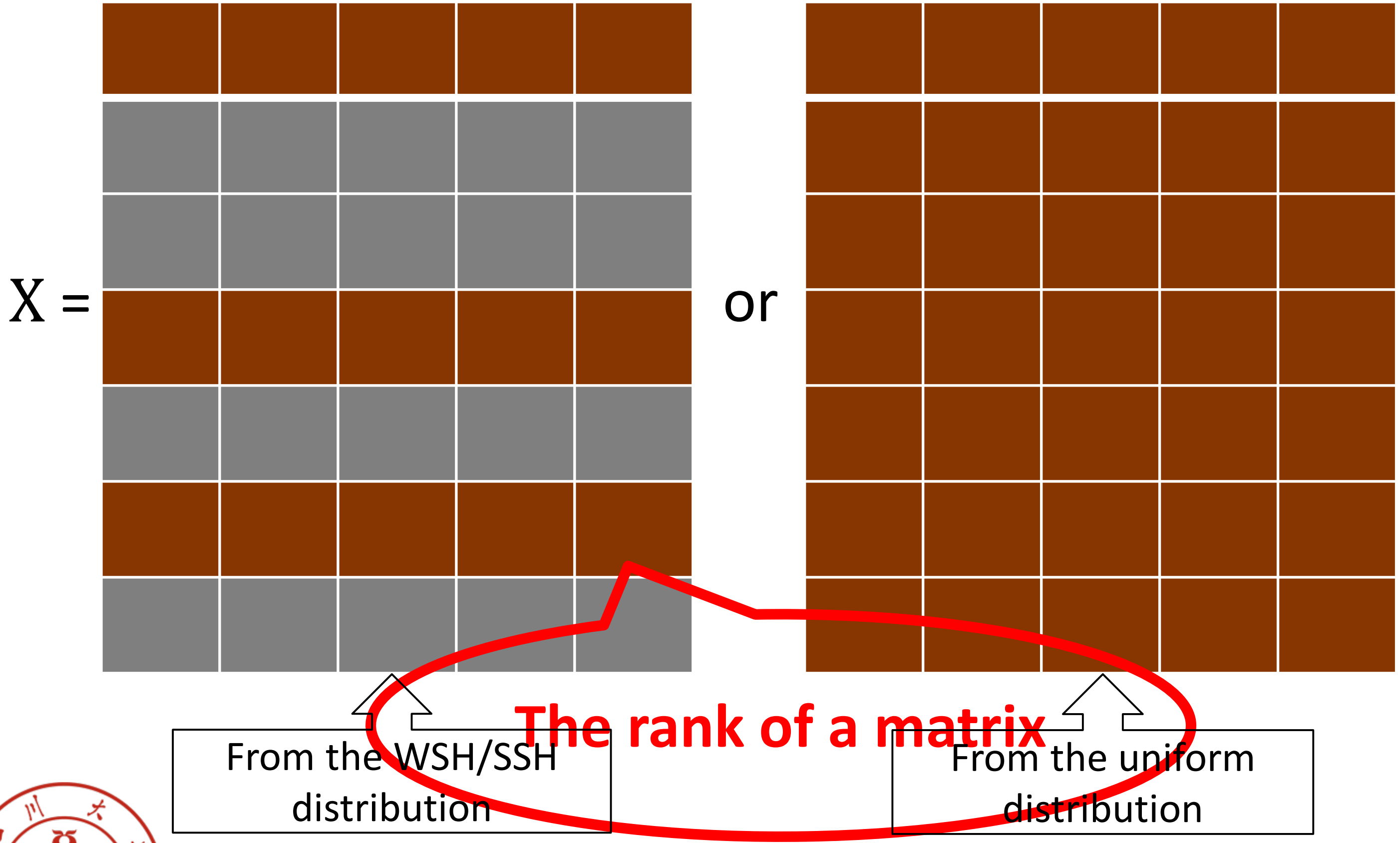
The Two-Server Case: Assume that the two servers do not collude and the decisional-WSH assumption holds. Then, the PVC protocol for matrix multiplication is private

The Single-Server Case: Assume that the decisional-SSH assumption holds. Then, the PVC protocol for matrix multiplication is private

Outline

Attack Strategy

- For a matrix X from either the WSH/SSH distribution or uniformly random, how to evaluate it using some special factor ?



Strategy Overview:

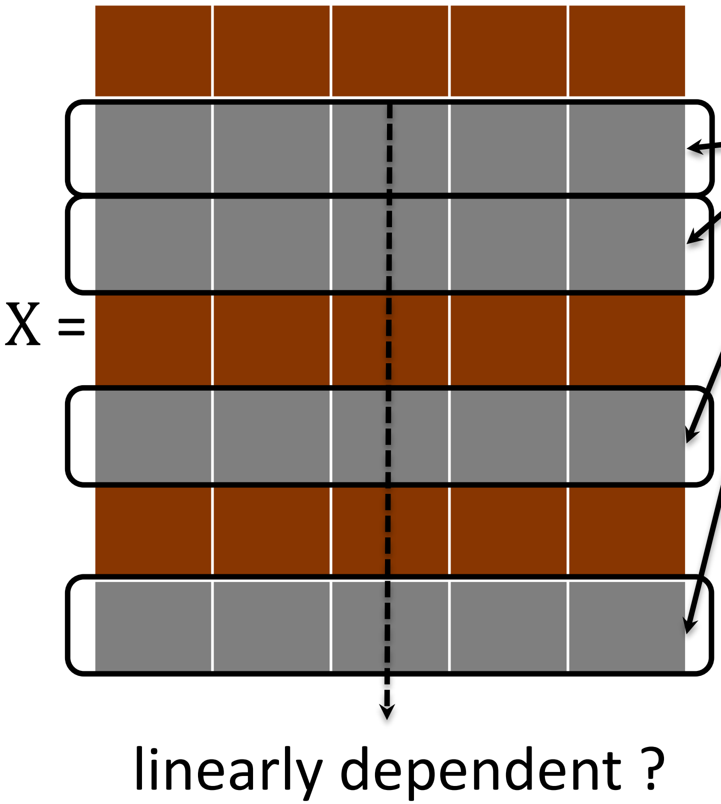
① Compute the rank of X

② Check whether the rank of X is below some value or not below this value

If the rank of X is below some value, X is sampled from the WSH/SSH distribution; otherwise, X is sampled from the uniform distribution

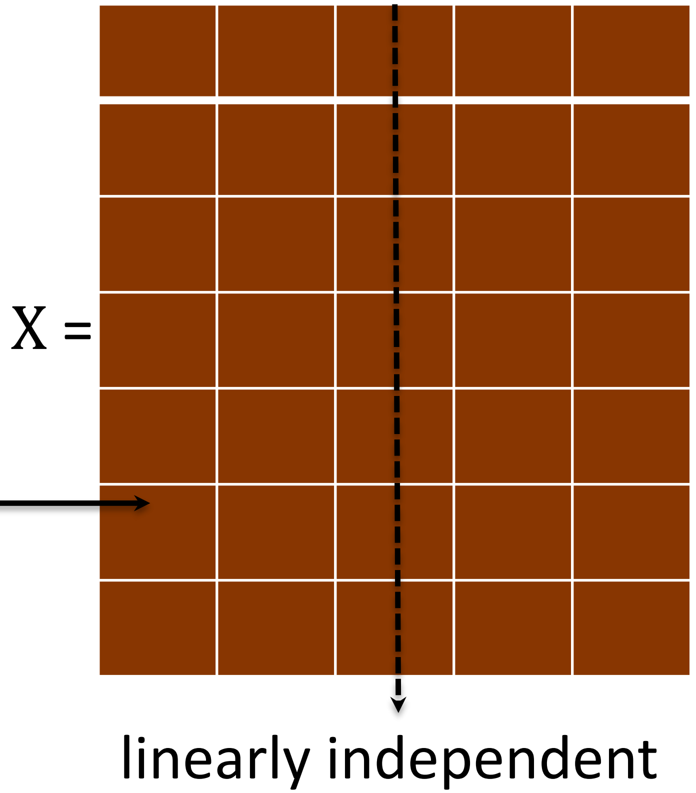
Attack Strategy

- Why the rank-based analysis works?



① *Fact 1:* If some row vectors in X are linearly dependent, all the row vectors of X are linearly dependent

② *Fact 2:* For a matrix X sampled from the uniform distribution, with high probability, all the row vectors of X are linearly independent

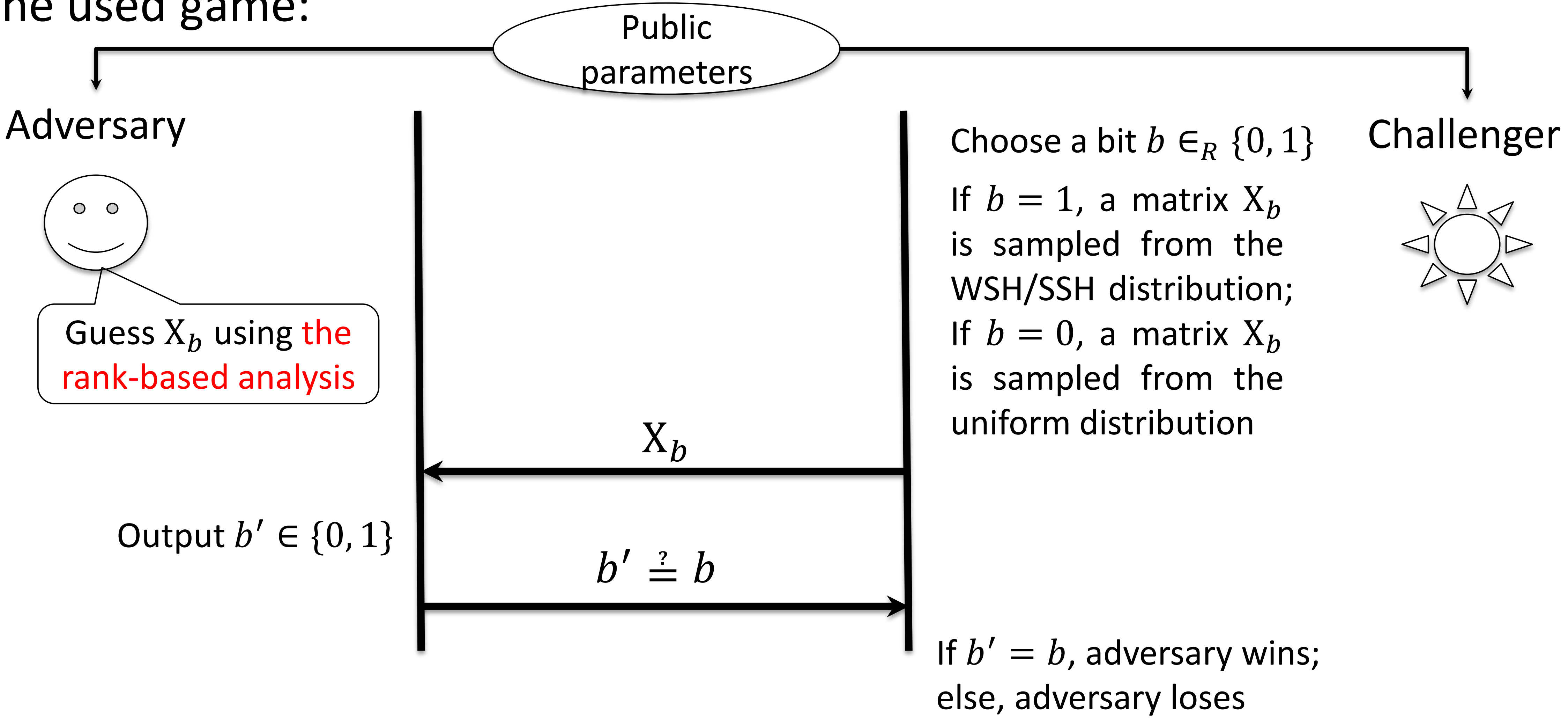


Outline

1. Background Information
2. Attack Strategy
3. Analysis for the Decisional Secret Hiding Assumption
4. Privacy Analysis for Atallah-Frikken Protocols
5. Experimental Verification

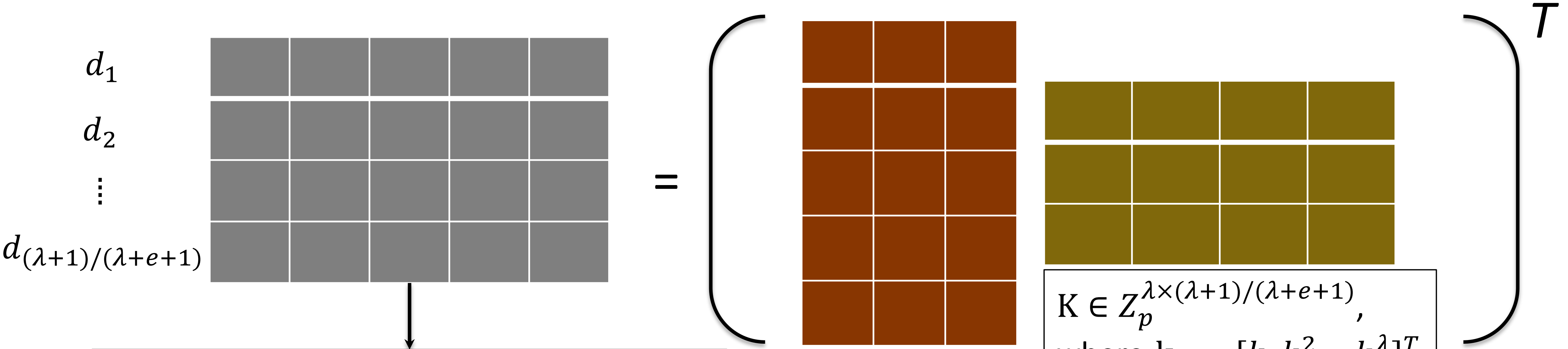
Analysis for the Decisional Secret Hiding Assumption

- The used game:



Analysis for the Decisional Secret Hiding Assumption

A significant motivation:



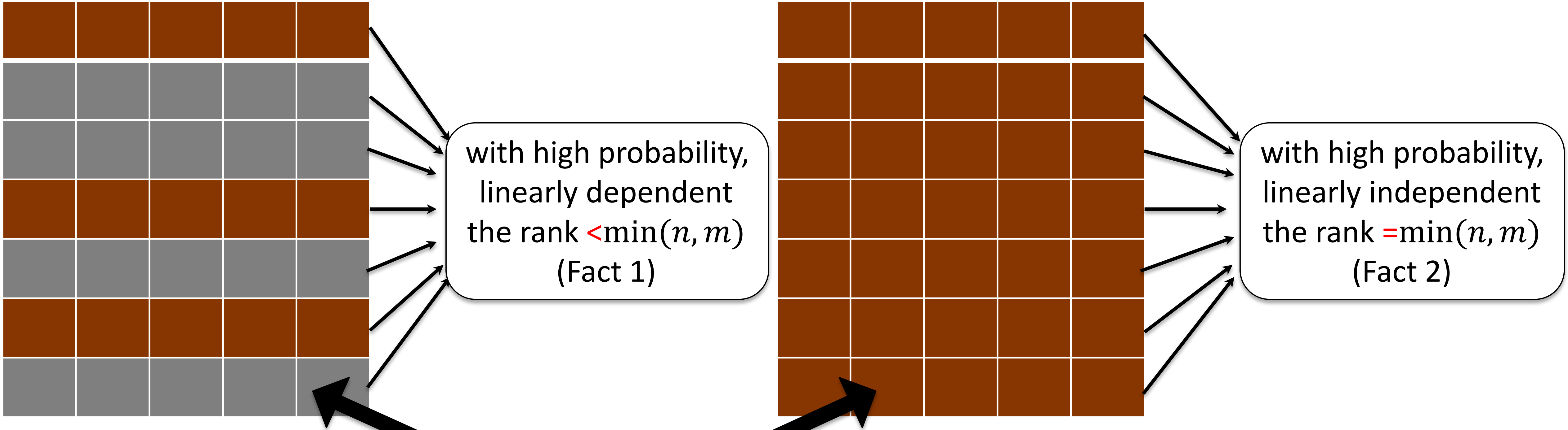
These row vectors $d_1, d_2, \dots, d_{(\lambda+1)/(\lambda+e+1)}$ are linearly dependent

Uniformly random matrix $A \in Z_p^{m\times\lambda}$

$K \in Z_p^{\lambda\times(\lambda+1)/(\lambda+e+1)}$, where $k_r = [k_r k_r^2 \dots k_r^{\lambda}]^T$, where $k_r \in Z_p^*, r \in [(\lambda + 1)/(\lambda + e + 1)]$

Analysis for the Decisional Secret Hiding Assumption

For the $n \times m$ matrix X_b:



Adversary can distinguish the samples from these two distributions with high probability!

Outline

1. Background Information

2. Attack Strategy

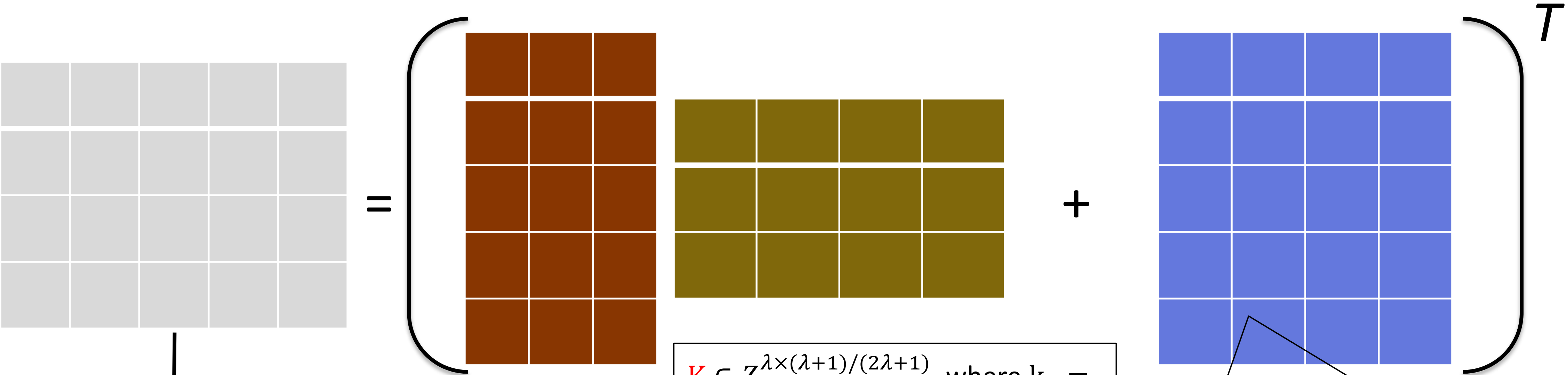
3. Analysis for the Decisional Secret Hiding Assumption

4. Privacy Analysis for Atallah-Frikken Protocols

5. Experimental Verification

Privacy Analysis for Atallah-Frikken Protocols

A significant motivation:



Uniformly random matrix $\color{red}{A} \in Z_p^{2v^2 \times \lambda}$

$\color{red}{K} \in Z_p^{\lambda \times (\lambda+1)/(2\lambda+1)}$, where $k_r = [k_r k_r^2 \ldots k_r^\lambda]^T$, where $k_r \in Z_p^*, r \in [(\lambda+1)/(2\lambda+1)]$

① $2v^2 \times (\lambda+1)/(2\lambda+1)$ matrix $\color{red}{S} = [s_1, s_1, \ldots s_1]$, where $s_1 \leftarrow_R Z_p^{2v^2}$

② $2v^2 \times (\lambda+1)/(2\lambda+1)$ zero matrix $\color{red}{Z}$

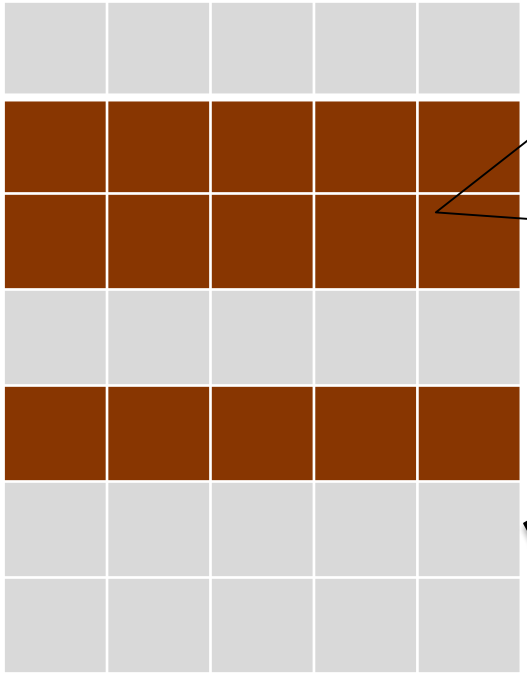
① The rank = $\lambda + 1$

② The rank < $\lambda + 1$

Privacy Analysis for Atallah-Frikken Protocols

For a COA-adversary (COA: Ciphertext-Only Attack):

- ✓ choose a matrix pair $(\mathrm{M}_{1(0)}, \mathrm{M}_{2(0)}) \leftarrow_R Z_p^{v\times v} \times Z_p^{v\times v}$ and a zero matrix pair $(\mathrm{M}_{1(1)}, \mathrm{M}_{2(1)})$
- ✓ use the rank-based analysis for the guess

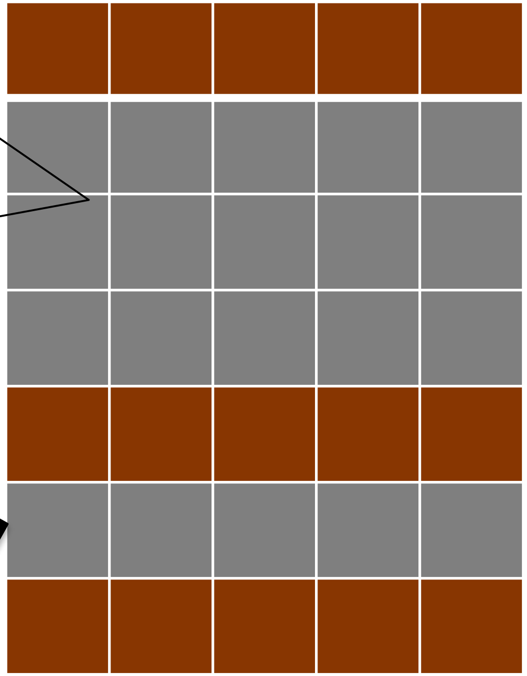


E_0

The rank = $(2\lambda + 1)/(3\lambda + 2)$. Then, this matrix involves all rows of $(\mathrm{AK} + \mathrm{S})^T$. This implies that the matrix pair is $(\mathrm{M}_{1(0)}, \mathrm{M}_{2(0)})$

distinguishable

The rank < $(2\lambda + 1)/(3\lambda + 2)$. Then, this matrix involves all rows of $(\mathrm{AK} + \mathrm{Z})^T$. This implies that the matrix pair is $(\mathrm{M}_{1(1)}, \mathrm{M}_{2(1)})$



E_1

with high probability, the COA-adversary can win the game by checking the rank of the combined ciphertext matrix $\stackrel{?}{=} (2\lambda + 1)/(3\lambda + 2)$

Outline

① Background Information

② Attack Strategy

③ Analysis for the Decisional Secret Hiding Assumption

④ Privacy Analysis for Atallah-Frikken Protocols

⑤ Experimental Verification

Experimental Verification

- Hardware and Software:
  - ✓ Lenovo ThinkStation (Intel(R) Xeon(R) E5-2620, 24 hyperthreaded cores at 2.00GHz, 8GB RAM at 2.00GHz)
  - ✓ Windows (Windows 7, x64_64)
  - ✓ NTL library version 10.5.0
- Parameters Choice:
  - ✓ $\lambda \in \{80,\ 128,\ 192,\ 256\}$
  - ✓ $e = h = \lambda,\ \ n \in \{2\lambda + 1,\ 2\lambda + 2e + 2\},\ \ m \in \{2\lambda + 1, 3\lambda + 1, 4\lambda + 2\},$ $p > 4\lambda + 2$
- Result:
  - ✓ Adversary's advantage
  - ✓ Cost

Experimental Verification

The experimental results confirm:

- ✓ Adversary can efficiently break the decisional WSH/SSH assumption with high advantage (i.e., adv.=0.5)
- ✓ COA-adversary can efficiently break the privacy of Atallah-Frikken PVC Protocols with high advantage (i.e., adv.=0.5)

Breaking the decisional WSH/SSH assumption

Our work

Breaking the privacy of Atallah-Frikken PVC Protocols

Breaking the decisional WSH/SSH assumption

Breaking the search variant of the WSH/SSH assumption

Summary

- Break the decisional WSH/SSH assumption
- Break the privacy of Atallah-Frikken PVC Protocols for matrix multiplication
- Give some experimental results to support the theoretical argument

Thank you !! Any question ?

E-mail: zhaoliangjapan@scu.edu.cn