IMPROVED (ALMOST) TIGHTLY-SECURE SIMULATION-SOUND QA-NIZK WITH APPLICATIONS

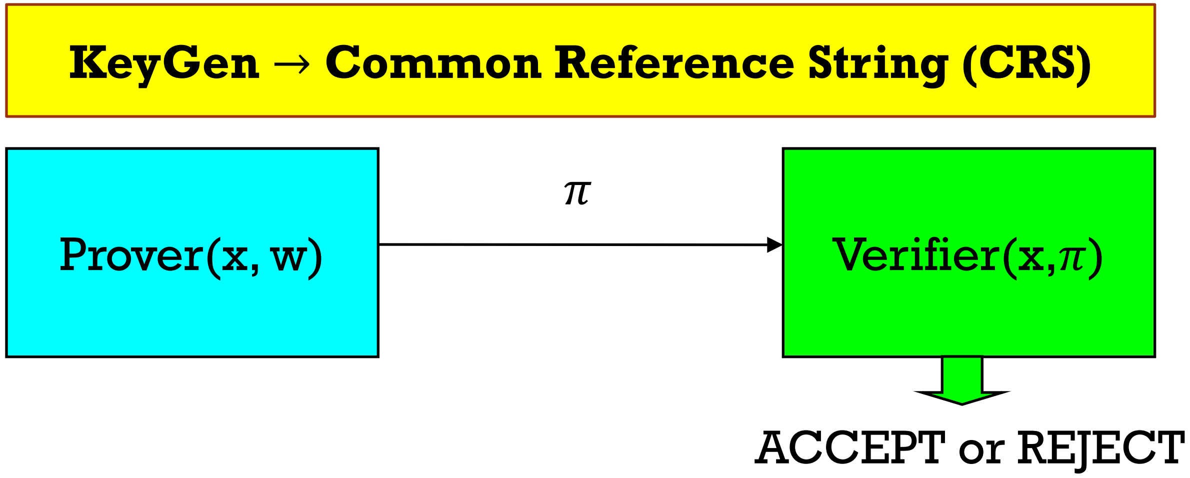
Masayuki Abe, Charanjit Jutla, Miyako Ohkubo and Arnab Roy

NTT Labs, IBM Research, NICT and Fujitsu Labs

Blum, Feldman, Micali
1988

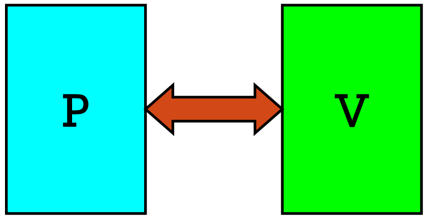
NIZK PROOF SYSTEMS

- Objective: To prove whether x $\in$ NP language L *without* revealing its witness w
- Components:



NIZK: PROPERTIES

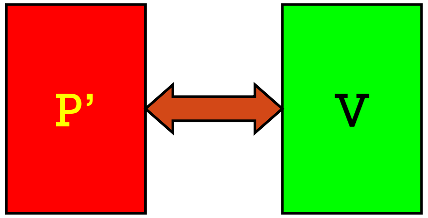
- Completeness



if $x \in L$ then V <u>accepts</u>

with 'high' probability

- Soundness



if $x \notin L$ then V <u>rejects</u>

with 'high' probability,

even with a cheating prover

ZERO-KNOWLEDGE

K		SimK
P	ZK $\approx$	Sim
V		V

Proofs from adversary are sound

~~Proofs from adversary are sound~~

Sahai 1999

UNBOUNDED SIMULATION-SOUND NIZK

K

P

V

ZK
≈

simK

Sim

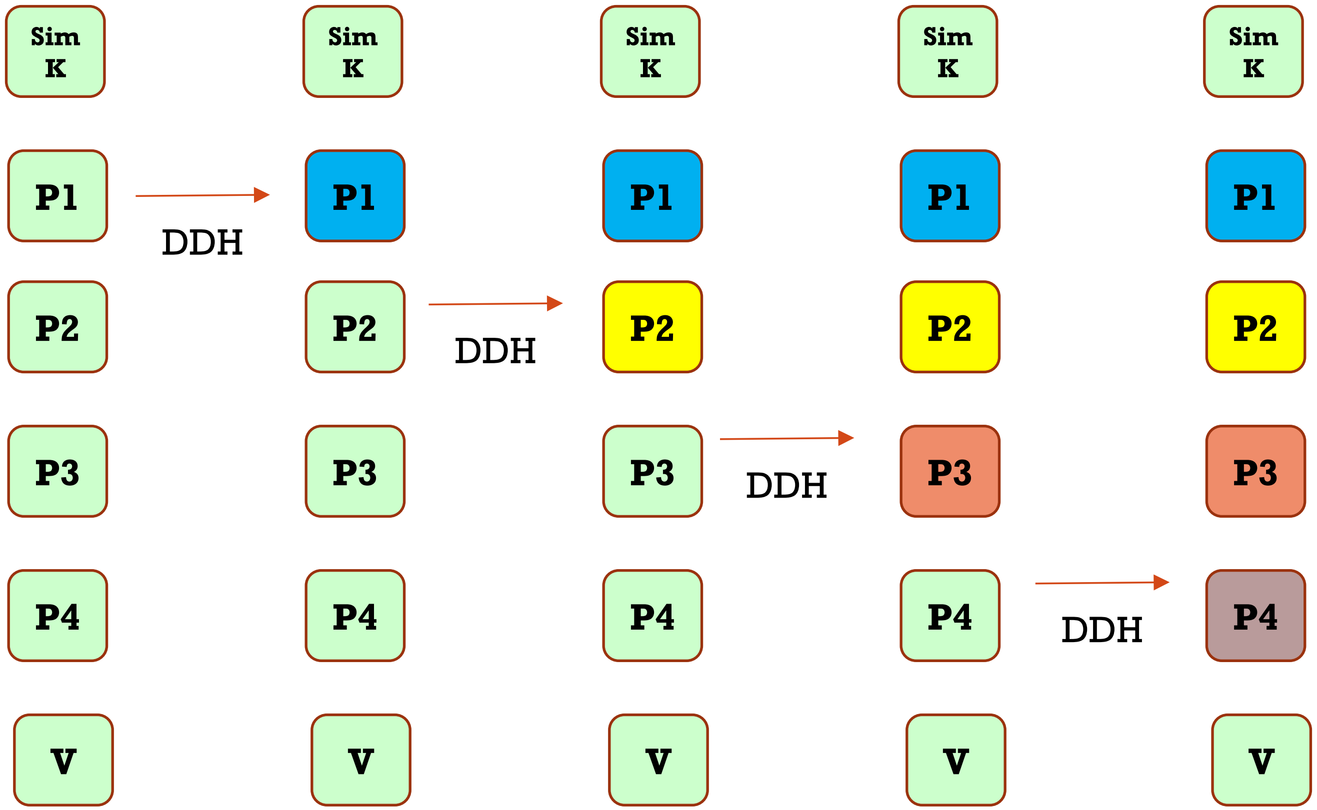
Any number of proofs

V

Proofs from adversary are sound

Proofs from adversary are sound

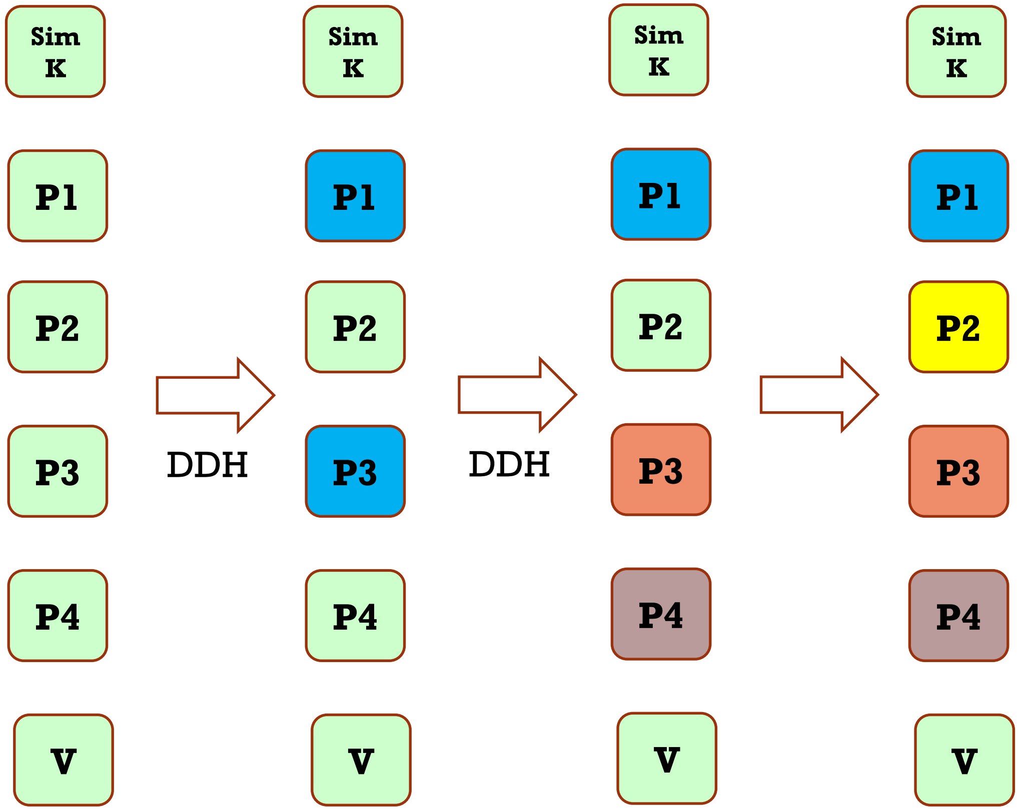
(NON)-TIGHT SECURITY



Proofs are transformed one by one.

O(Q) reduction to DDH

(ALMOST)-TIGHT SECURITY

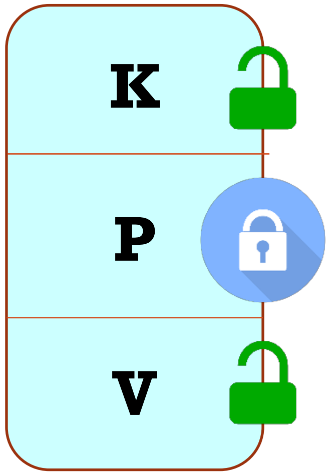


Many proofs are transformed in one go.

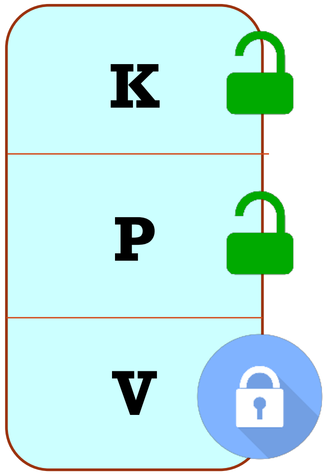
$O(\lambda, \log Q)$ reduction to DDH.

WHY IS THIS CHALLENGING?

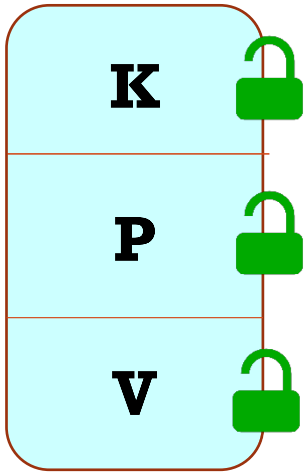
Signatures



PKEs



NIZK



Jutla-R 2013, Kiltz-Wee 2015

QUASI-ADAPTIVE NIZKS

Smooth Projective Hash Functions [CS98]

$y = [Mx]$
$y^T = [x^T M^T]$

Proj. Hash Key
$[M^T K]$

Hash Key
K

Public Hash
$x^T [M^T K]$

Private Hash
$y^T K$

QA-NIZKs

$y = [Mx]_1$
$y^T = [x^T M^T]_1$

CRSp
$[M^T K]_1$

Trapdoor
K

CRSv
$[KA]_2, [A]_2$

Proof
$p = x^T [M^T K]_1$

Simulator
$y^T K$

Verify
$y^T [KA]_2$
$= p[A]_2$

Kiltz-Wee 2015

USS-QA-NIZK

- QA-NIZKs
- USS-QA-NIZKs

$$y = [Mx]_1$$
$$y^T = [x^T M^T]_1$$

Proof
$$p = x^T [M^T K]_1$$

+

PR-MAC
$$+[r^T (P_0 + \tau P_1)]_1,$$
$$[r^T B^T]_1$$

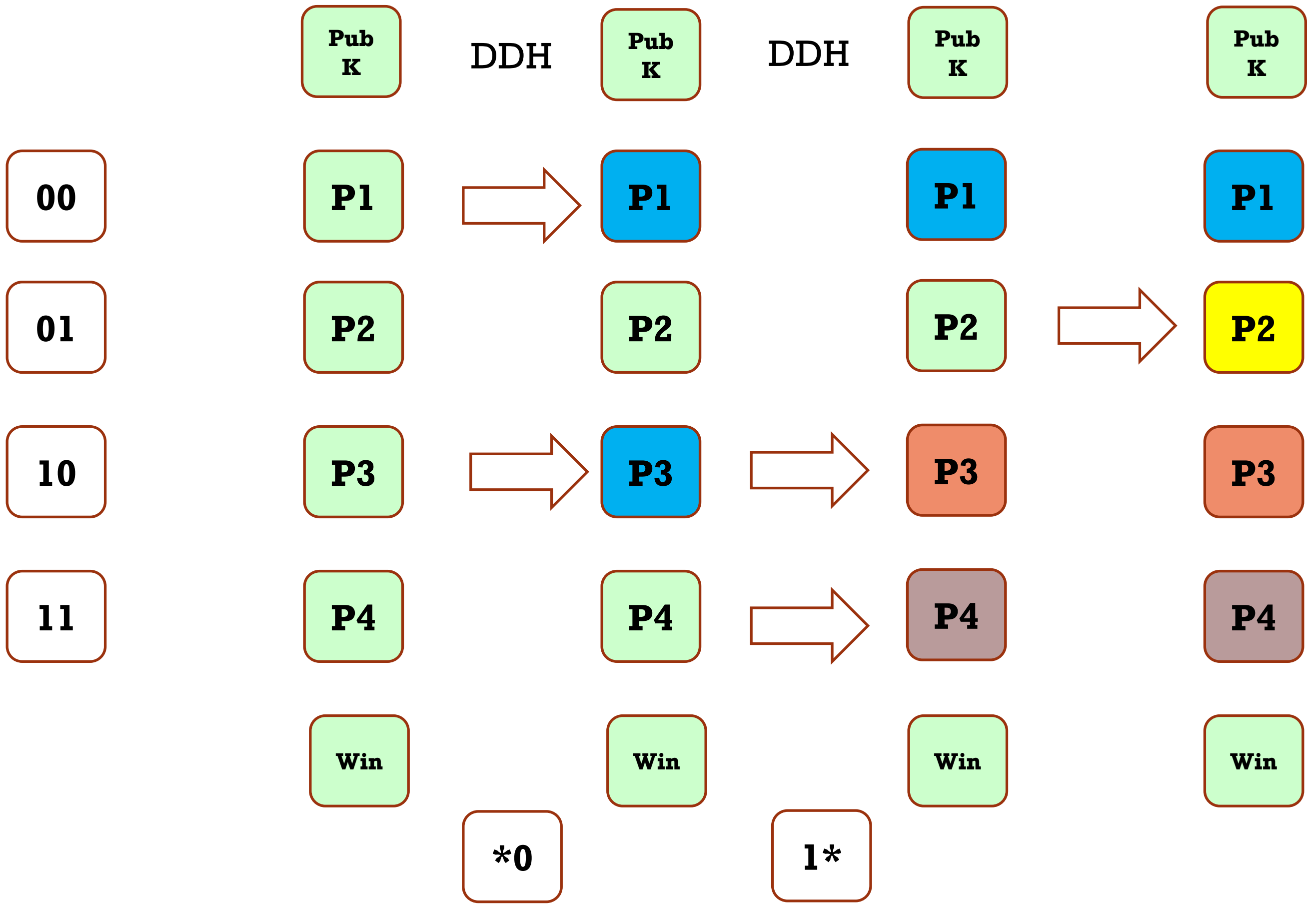
Non-tight
O(Q) reduction

TIGHTLY-SECURE USS-QA-NIZK

- [LPJY15] achieved this first
  - #proof independent of λ
  - $O(\lambda)$ security reduction to DLIN
  - Public key size $O(\lambda)$
  - Static partitioning [CW13, …]
- We improve in the following ways
  - $O(\log Q)$ security reduction to any MDDH including SXDH
  - #Public key also independent of λ
  - Adaptive partitioning [Hof17, used by: AHN+17, JOR18, GHKP18, …]

Hofheinz 2017, GHKP 2018

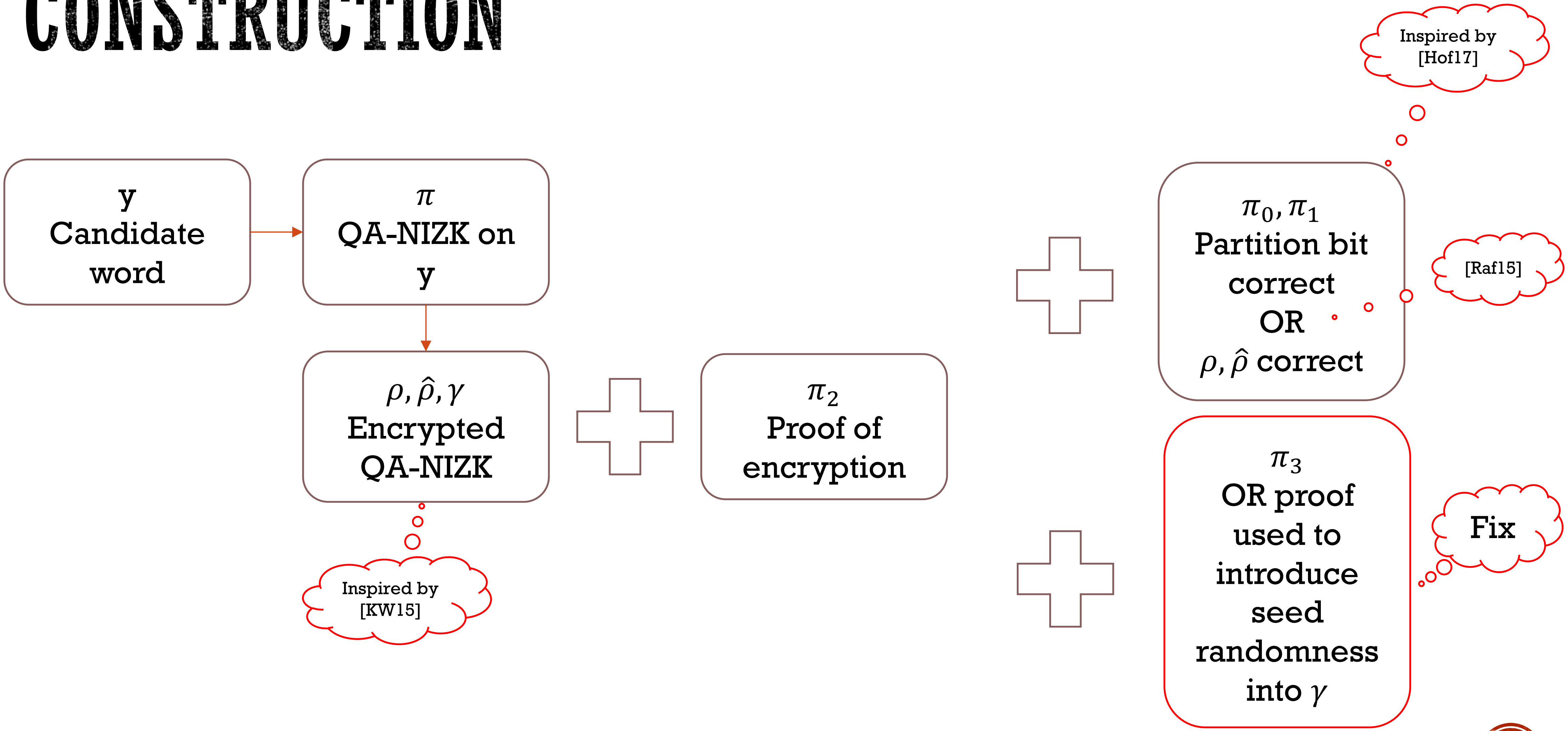
ADAPTIVE PARTITIONING



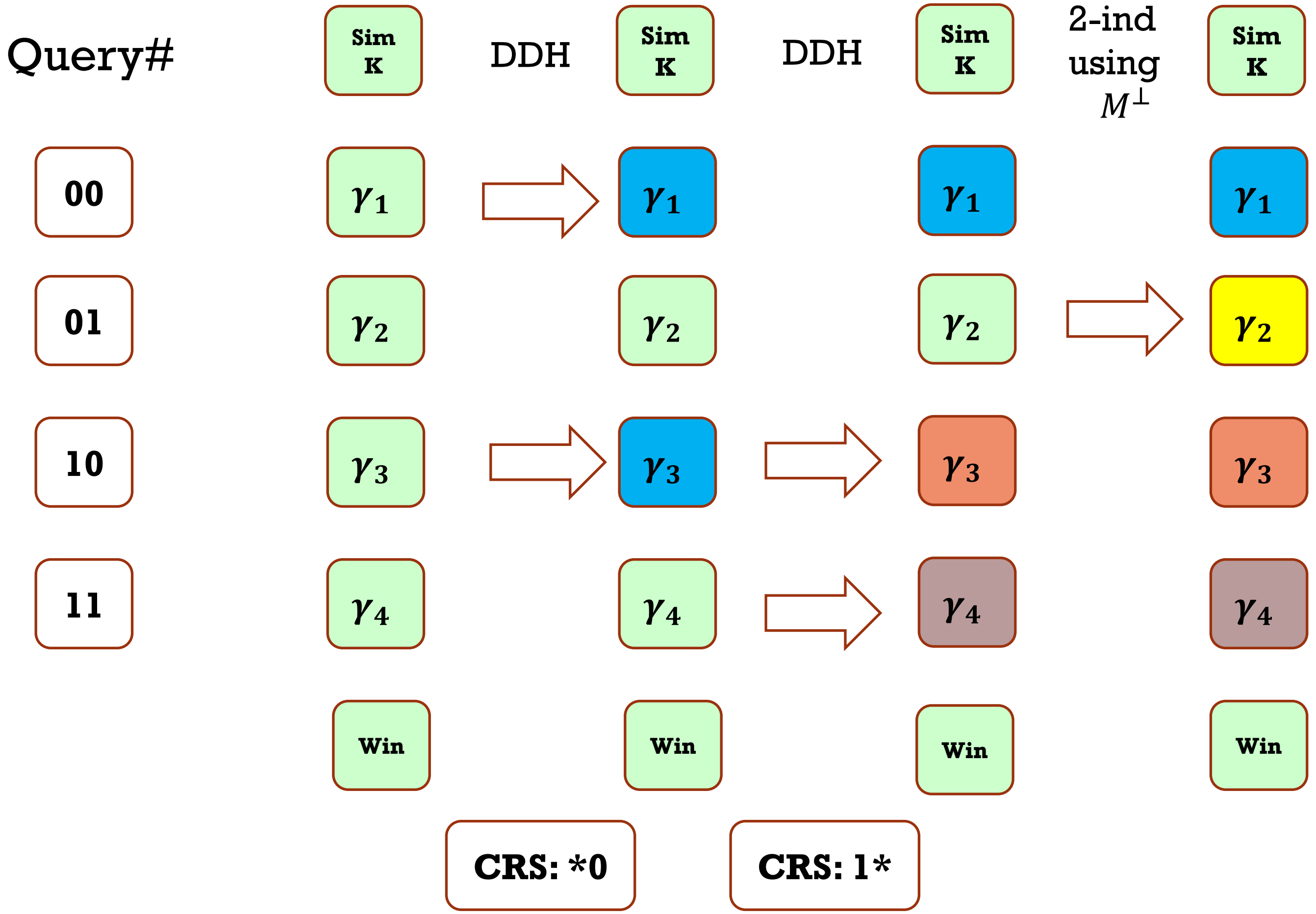
TIGHT USS-QA-NIZK CONSTRUCTION

- Our AsiaCrypt version had a bug
- Jiaxin Pan discovered an attack and informed us
  - Thanks Jiaxin!
- Today I will present a fixed construction
  - On the negative side it is longer
  - On the positive side, the structure-preserving version is also $O(\log Q)$-tight
    - Previously it was only $O(\lambda)$-tight
  - The designated prover version is not impacted by this bug, so SPS is OK.
  - Ongoing work:
    - While working on the fixes, we could reduce the tight-SPS size from 12 to 10
  - Revised version will be updated in eprint soon

CONSTRUCTION



PROOF STRATEGY



$\rho, \hat{\rho}, \gamma$
Encrypted
QA-NIZK

π_0, π_1
Partition bit
correct
OR
$\rho, \hat{\rho}$ correct

SUMMARY

- First USS-QA-NIZK where both CRS and proofs have number of group elements independent of the security parameter
- Shortest tightly secure SPS with 12 group elements under SXDH
  - Ongoing optimization work on 10 group elements
- Shortest public-verifiable tightly-secure CCA scheme
- Plugging our USS-QA-NIZK gives short tightly-secure primitives
  - Blind Structure-Preserving Signatures
  - Group Structure-Preserving Signatures
  - USS Groth-Sahai Proof System

THANK YOU!

Questions?