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
NIZK PROOF SYSTEMS

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

KeyGen $\rightarrow$ Common Reference String (CRS)

Prover($x, w$) $\rightarrow$ Verifier($x, \pi$)

$\pi$ $\rightarrow$ ACCEPT or REJECT

Blum, Feldman, Micali 1988
**NIZK: PROPERTIES**

- **Completeness**

  if $x \in L$ then $V$ accepts with 'high' probability

- **Soundness**

  if $x \notin L$ then $V$ rejects with 'high' probability, even with a cheating prover
Zero-Knowledge

Proofs from adversary are sound
UNBOUNDED SIMULATION-SOUND NIZK

Proofs from adversary are sound

Proofs from adversary are sound

Sahai 1999
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
Smooth Projective Hash Functions [CS98]

\[ y = [Mx] \]
\[ y^T = [x^TM^T] \]

QA-NIZKs

\[ y = [Mx]_1 \]
\[ y^T = [x^TM^T]_1 \]

- Proj. Hash Key: \([M^TK]\)
- Hash Key: \(K\)
- Public Hash: \(x^T[M^TK]\)
- Private Hash: \(y^TK\)
- CRSp: \([M^TK]_1\)
- Trapdoor: \(K\)
- CRSpv: \([KA]_2, [A]_2\)
- Proof: \(p = x^T[M^TK]_1\)
- Simulator: \(y^TK\)
- Verify: \(y^T[KA]_2 = p[A]_2\)
USS-QA-NIZK

- QA-NIZKs
  \[ y = [Mx]_1 \]
  \[ y^T = [x^T M^T]_1 \]

- USS-QA-NIZKs
  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

Kiltz-Wee 2015
Tightly-Secure USS-QA-NIZK

- [LPJY15] achieved this first
  - #proof independent of $\lambda$
  - $O(\lambda)$ 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 $\lambda$
  - Adaptive partitioning [Hof17, used by: AHN+17, JOR18, GHKP18, …]
ADAPTIVE PARTITIONING

Hofheinz 2017, GHKP 2018

Win

Pub
K

DDH

P1

00

P2

01

P3

10

P4

11

Win

*0

1*

Pub
K

DDH

P1

P1

P1

P1

Pub
K

Pub
K

Pub
K

Pub
K

Hofheinz 2017, GHKP 2018
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

\( y \quad \text{Candidate word} \)

\( \pi \quad \text{QA-NIZK on } y \)

\( \rho, \hat{\rho}, \gamma \quad \text{Encrypted QA-NIZK} \)

\( \pi_2 \quad \text{Proof of encryption} \)

\( \pi_0, \pi_1 \quad \text{Partition bit correct} \)

\( \rho, \hat{\rho} \quad \text{correct} \)

\( \pi_3 \quad \text{OR proof used to introduce seed randomness into } \gamma \)

Inspired by [KW15], [Hof17], [Raf15]
PROOF STRATEGY

<table>
<thead>
<tr>
<th>Query#</th>
<th>Sim K</th>
<th>DDH</th>
<th>Sim K</th>
<th>DDH</th>
<th>Sim K</th>
<th>2-ind using $M^\perp$</th>
<th>Sim K</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>$\gamma_1$</td>
<td>$\gamma_1$</td>
<td>$\gamma_1$</td>
<td>$\gamma_1$</td>
<td>$\gamma_1$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>01</td>
<td>$\gamma_2$</td>
<td>$\gamma_2$</td>
<td>$\gamma_2$</td>
<td>$\gamma_2$</td>
<td>$\gamma_2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>$\gamma_3$</td>
<td>$\gamma_3$</td>
<td>$\gamma_3$</td>
<td>$\gamma_3$</td>
<td>$\gamma_3$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>$\gamma_4$</td>
<td>$\gamma_4$</td>
<td>$\gamma_4$</td>
<td>$\gamma_4$</td>
<td>$\gamma_4$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Encrypted QA-NIZK

$\rho, \hat{\rho}, \gamma$

$\pi_0, \pi_1$
Partition bit correct
OR
$\rho, \hat{\rho}$ correct

CRS: *0
CRS: 1*
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!