Bar-Ilan University
אוניברסיטת בר-אילן
BIU Center for Research in Applied Cryptography and Cyber Security
The 11th BIU Winter School on Cryptography in a Quantum World
February 14-17, 2021

Thomas Vidick
California Institute of Technology

Delegation of quantum computations

Thomas Vidick, Caltech

Part III: *Delegation with a classical verifier and a computationally bounded server*

The Morimae-Fitzsimons protocol

Theorem. *For any* $n \geq 1$ *there is* $m = \text{poly}(n)$ *such that the following holds. Given a poly-size quantum circuit* $\mathcal{C}$ *acting on* n *qubits and an input* x *for* $\mathcal{C}$ *there exist efficiently computable real weights* $\{\alpha_P : P \in \{I, X, Z\}^{\otimes m}\}$ *such that* $\sum_P |\alpha_P| = 1$ *and moreover if*

$$H_{\mathcal{C}} = \sum_{P \in \{I,X,Z\}^{\otimes m}} \alpha_P P$$

then:

- *(Completeness) If* $\mathcal{C}$ *accepts* x *with probability at least* $2/3$ *then* $\lambda_{min}(H_{\mathcal{C}}) \leq -\frac{2}{3}$*;*
- *(Soundness) If* $\mathcal{C}$ *accepts* x *with probability at most* $1/3$ *then* $\lambda_{min}(H_{\mathcal{C}}) \geq \frac{2}{3}$*.*

Claw-free functions

Definition (Trapdoor claw-free function family)**.**

A family $\mathcal{F} = \{f_{pk} : \{0,1\}^{m(\lambda)} \to \{0,1\}^{m(\lambda)}\}_{pk \in \{0,1\}^{k(\lambda)}}$ *is* trapdoor claw-free *against classical (resp. quantum) adversaries if the following conditions hold:*

- *There is a PPT key generation procedure* $(pk, td) \leftarrow \textsc{Gen}(1^\lambda)$.

- f_{pk} *can be efficiently evaluated: there is a PPT procedure that given pk and x as inputs returns* $f_{pk}(x)$.

- *For every* $\lambda \in \mathbb{N}$ *and* $pk \in \{0,1\}^{k(\lambda)}$, f_{pk} *is* 2*-to-*1*. Moreover, for any* y *in the range of* f_{pk} *the two preimages of* y *take the form* (b, x_b) *where* $b \in \{0,1\}$ *and* $x_b \in \{0,1\}^{m(\lambda)-1}$.

- *For every PPT (resp. QPT) procedure* $\mathcal{A}$ *there is a negligible function* $\mu : \mathbb{N} \to \mathbb{N}$ *such that for every* λ,

$$\Pr_{pk \leftarrow_R \{0,1\}^{k(\lambda)}} \big((x_0, x_1) \leftarrow \mathcal{A}(1^\lambda, pk) : \; x_0 \neq x_1, \; f_{pk}(x_0) = f_{pk}(x_1)\big) \; \leq \; \mu(\lambda) \, .$$

- *Given pk, td and any* y *in the range of* f_{pk} *it is possible to efficiently recover the two preimages* x_0 *and* x_1 *of* y.

Committing to a qubit

Let $f : \{0,1\}^m \to \{0,1\}^m$ be claw-free. Let $|\phi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$ be a qubit.

The Mahadev protocol (single qubit)

Let $\mathcal{F}$ be a trapdoor claw-free function family and $\lambda \in \mathbb{N}$ a security parameter. Let $\gamma = 0$. Let $H = \alpha_X X + \alpha_Z Z$. Repeat N times:

1. The verifier generates $(pk, td) \leftarrow \textsc{Gen}(1^\lambda)$. It sends pk to the prover.

2. The prover returns $y \in \{0,1\}^m$.

3. The verifier selects a uniformly random challenge $c \leftarrow_R \{0,1\}$ and sends c to the prover.

4. (a) *(Computational basis, $c = 0$:)* In case $c = 0$ the prover is expected to return $(b, x) \in \{0,1\}^m$. If $f(b, x) \neq y$ then the verifier aborts. The verifier sets $a_Z \leftarrow (-1)^b$ and $\gamma \leftarrow \gamma + \alpha_Z a_Z$.

   (b) *(Hadamard basis, $c = 1$:)* In case $c = 1$ the prover is expected to return $(u, d) \in \{0,1\}^m$. The verifier uses td to determine the two preimages (b, x_b) of y. She sets $a_X \leftarrow (-1)^u \cdot (-1)^{d \cdot (x_0 + x_1)}$ and $\gamma \leftarrow \gamma + \alpha_X a_X$.

If the verifier has not aborted at any of the steps $c = 0$, she returns the real number $o = \frac{2}{N}\gamma$.

Soundness analysis

Suppose P succeeds with probability 1 in the preimage test.

Definition (Extracted qubit)**.**

Lemma (The isometry). *Let $\hat{Z}$, $\hat{X}$ be observables on $\mathcal{H}$. Let $|\psi\rangle \in \mathcal{H}$. Define*

$$\begin{aligned} V : \mathcal{H} &\mapsto (\mathcal{H} \otimes \mathbb{C}_2) \otimes \mathbb{C}^2 \\ |\psi\rangle &\mapsto \frac{1}{2}(\mathrm{Id} \otimes \mathrm{Id} \otimes \mathrm{Id} + \hat{X} \otimes X \otimes \mathrm{Id} + \hat{Z} \otimes Z \otimes \mathrm{Id} + \hat{X}\hat{Z} \otimes XZ \otimes \mathrm{Id})(|\psi\rangle \otimes |EPR\rangle_{AB}) \end{aligned}$$

Definition (Extracted qubit). *For any prover P and string y, define the extracted qubit*

$$\rho = \mathrm{Tr}_{\mathcal{H}'A}\left(V|\psi_y\rangle\langle\psi_y|V^{\dagger} \right).$$

Lemma. *Suppose* P *succeeds with probability one in the preimage test. Let* ρ *be the extracted qubit. Then*

- *(Z-measurement:) The outcome of measuring* ρ *in the computational basis is identically distributed to the bit* $(-1)^b$ *computed from the prover's answer* x *in case* $c = 0$*.*

- *(X-measurement:)* **(**)** *The outcome of measuring* ρ *in the Hadamard basis is computationally indistinguishable from the bit* $(-1)^{u+d\cdot(x_0+x_1)}$ *computed from the prover's answer* x *in case* $c = 1$*.*

Definition (Adaptive hardcore bit)**.** *Let* $\mathcal{F}$ *be a* 2*-to-*1 *trapdoor claw-free function family. For any QPT adversary* $\mathcal{A}$ *there is a negligible function* μ *such that*

$$\left|\frac{1}{2} - \Pr_{pk \leftarrow_R \{0,1\}^{k(\lambda)}}\Big((x,d) \leftarrow \mathcal{A}(1^\lambda, pk),\ \{x_0, x_1\} \leftarrow f_{pk}^{-1}(f_{pk}(x)) :\ d \neq 0^m \wedge d \cdot (x_0 + x_1) = 0\Big)\right| \leq \mu(\lambda)\,.$$

Summary

- Prover that succeeds with probab. 1 in preimage test ("perfect prover") leads to an outcome o recorded by the verifier s.t. $\mathrm{E}[o] \approx_c \langle\phi|H|\phi\rangle$ for some $|\phi\rangle$ (or the prover breaks the hardcore bit assumption).

- Sequential repetition to estimate o + simple reduction to perfect prover gives constant completeness/soundness gap

- Extension to multiqubit H requires additional assumptions:

  - "Collapsing" property for multiqubit $X \cdots X$ or $Z \cdots Z$ terms.

  - Mixed XZ terms require more challenges and additional "injective invariance" property.

  - Independent keys used to "commit" to each qubit.

- Final 4-message protocol has completeness negligibly close to 1 and soundness $3/4$.

Extensions and open questions

- Extensions:
  - [Alagic-CGH'20] Non-interactive protocol in QRO model
  - [Chia-CY'20] Make verifier super-efficient using CRS+QRO
  - [Chung-LLW'21] Consider sampling problems
  - [V-Zhang'20] Proof of quantum knowledge property
- [Georghiu-V'19] Remote state preparation $\rightarrow$ composable protocol, measurement-based model
- Open questions:
  - 1-round protocol
  - Different assumptions. Information-theoretic security?
  - Verification of restricted classes of circuits/ restricted provers