Commitments are equivalent to statistically verifiable one-way state generators

Rahul Jain

Centre for Quantum Technologies
National University of Singapore

Joint work with Rishabh Batra (CQT, NUS)

FOCS 2024; TQC 2025; QCrypt 2024; ArXiv:2308.07340

Commitments

- One of the most fundamental primitives in cryptography.
- 2 parties: a sender and a receiver.
- Commit phase: the sender commits to some message m to the receiver.
- Reveal phase: the sender reveals m to the receiver.
- We want:
  1. **Hiding**: the receiver should not be able to learn m during the commit phase.
  2. **Binding**: the sender should not be able to reveal $m' \neq m$ during the reveal phase.

One-Way Functions (OWF)

Classical one-way functions

A function $f : \{0,1\}^n \to \{0,1\}^m$

- efficiently computable
- hard to invert by a (non-uniform) PPT (probabilistic polynomial time) adversary
- OWF are equivalent to commitments, pseudorandom generator (PRG), pseudorandom function (PRF)

Quantum-secure one-way functions

A function $f : \{0,1\}^n \to \{0,1\}^m$

- efficiently computable
- hard to invert by a (non-uniform) QPT (quantum polynomial time) adversary

Can we do anything more in the quantum world?

Quantum One-Way State Generator (OWSG) [MY22]

An *m*-copy one-way state generator (OWSG) is a set of algorithms (here λ is the security parameter):

1. $\textsc{KeyGen}(1^\lambda) \to x$: a PPT algorithm that outputs a classical key $x \in \{0,1\}^n$.
2. $\textsc{StateGen}(1^\lambda, x) \to \phi_x$: a QPT algorithm that outputs a (mixed) quantum state ϕ_x corresponding to the key x.
3. $\textsc{Ver}(1^\lambda, x', \theta) \to \top/\bot$: a QPT algorithm that on input a string x' and a state θ gives as output $\top$ or $\bot$.

statistically verifiable (sv)-OWSG: $\textsc{Ver}$ may not be efficient.

OWSG

Correctness

$$\Pr[x \leftarrow \textsc{KeyGen}(1^\lambda), \phi_x \leftarrow \textsc{StateGen}(1^\lambda, x), \top \leftarrow \textsc{Ver}(1^\lambda, x, \phi_x)]$$
$$\geq 1 - \mathsf{negl}(\lambda).$$

Security
For any (non-uniform) QPT adversary $\mathcal{A}$,

$$\Pr[x \leftarrow \textsc{KeyGen}(1^\lambda), \phi_x \leftarrow \textsc{StateGen}(1^\lambda, x), x' \leftarrow \mathcal{A}(1^\lambda, \phi_x^{\otimes m}),$$
$$\top \leftarrow \textsc{Ver}(1^\lambda, x', \phi_x)] = \mathsf{negl}(\lambda).$$

Note: $\textsc{Ver}$ needs 1 additional copy of the state ϕ_x to verify.

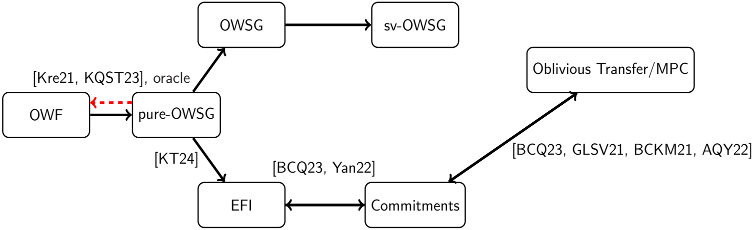
Efficiently samplable, statistically Far, computationally Indistinguishable pair of quantum states (EFI) [BCQ23]

EFI generator: a QPT algorithm $\textsc{StateGen}(1^\lambda, b) \to \rho_b$

1. $\rho_0 \approx_{\mathsf{negl}_C} \rho_1$.
2. ρ_0 and ρ_1 are statistically distinguishable with noticeable advantage, that is, $\frac{1}{2}\left\|\rho_0 - \rho_1\right\|_1$ is a noticeable function in λ.

We call (ρ_0, ρ_1) an EFI pair.

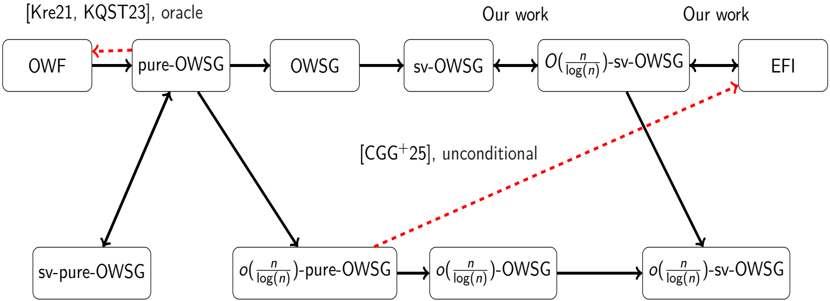
Motivation



- EFI-pairs imply oblivious transfer and secure-multi-party computation.
- There is an oracle separation between pure-OWSG and quantum-secure one-way functions. Hence, pure-OWSG are potentially weaker objects than OWF [Kre21, KQST23].

What is the weakest OWSG from which we can get EFI?

Our results



[Kre21, KQST23], oracle
Our work
Our work
OWF
pure-OWSG
OWSG
sv-OWSG
$O(\frac{n}{\log(n)})$-sv-OWSG
EFI
[CGG+25], unconditional
sv-pure-OWSG
$o(\frac{n}{\log(n)})$-pure-OWSG
$o(\frac{n}{\log(n)})$-OWSG
$o(\frac{n}{\log(n)})$-sv-OWSG

HILL: OWF $\implies$ EFI

- Assume f is a one-way permutation.
- Let g be a hardcore function of output length $O(\log n)$.
- EFI
  - $(P, Q) = (f(X)Rg(X, R), f(X)R \otimes U_{|g(X,R)|})$
  - since g is hardcore: $P \approx_{\mathsf{negl}_C} Q$
  - since f is injective: $S(P) + O(\log n) \leq S(Q)$ and hence (P, Q) are statistically far
  - (P, Q) are efficiently samplable

HILL: OWF $\implies$ EFI

- f is OWF.
- H is seed and $H^l(X)$ is l-bit output of a seeded extractor.
- Append $HH^l(X)$: $\quad (X,H) \to f(X)HH^l(X)$
  - extracts residual entropy in X given $f(X)$
  - $(X,H) \to f(X)HH^l(X)$ (sort of) an injective function
  - requires $l \approx S(X|f(X))$ ($\approx$ means up to additive $O(\log n)$)
  - need to ensure $(X,H) \to f(X)HH^l(X)$ is OWF
  - need $f(X)HH^l(X) \approx_{\mathrm{negl}_C} f(X) \otimes H \otimes U_l$
  - forces $l \approx S_2(X|f(X))$ (collision entropy)
  - X conditioned on $f(X)$ is flat: $S(X|f(X)) = S_2(X|f(X))$
  - l depended on $f(X)$; finding l from $f(X)$ not efficient
  - handled this via intricate, elaborate arguments

HILL: OWF $\implies$ EFI

- EFI
  - $(P, Q) = (f(X)HH^{\ell}(X)Rg(X, R), f(X)HH^{\ell}(X)R \otimes U_{|g(X,R)|})$
  - since g is hardcore: $P \approx_{\text{negl}_C} Q$
  - injectivity ensures P and Q are statistically far
  - (P, Q) are efficiently samplable
- PRG
  - $(X^{\otimes t}, H^{\otimes t}, R^{\otimes t}, S_1, S_2) \to \text{Ext}(X^{\otimes t}, S_2)\ \text{Ext}(P^{\otimes t}, S_1)$
  - Ext: seeded extractor
  - determining output lengths of the extractors is not efficient
  - handled via **stretching** the output of PRG

Quantum case issues

- cannot condition on a quantum state
- multiple copies of $f(x)$ to adversary have to be handled
- do not know how to stretch the output

Imbalanced EFI [KT24]

An s^*-imbalanced EFI: a QPT algorithm $\mathsf{EFI}_s(1^\lambda, b) \to \rho_b(s)$ (s is advice string)

1. For all $s \leq s^*$: $\rho_0(s) \approx_{\mathsf{negl}_C} \rho_1(s)$ (computational indistinguishability).
2. For all $s \geq s^*$: $\rho_0(s)$ and $\rho_1(s)$ are statistically distinguishable with noticeable advantage, that is $\frac{1}{2}\left\|\rho_0(s) - \rho_1(s)\right\|_1$ is a noticeable function in λ.

- We show a construction of imbalanced-EFI from sv-OWSG.
- We use [KT24] for imbalanced-$\mathrm{EFI} \implies \mathrm{EFI}$.

Our construction: Imbalanced-EFI from sv-OWSG

$\mathbf{EFI}_k(1^\lambda, b)$

1. Input: security parameter λ and a bit b.
2. Subroutine: an m-copy sv-OWSG with key-length n that generates a one-way state τ^{XQ^m}.
3. For all $i \in [m], l \in [n]$ (g is a quantum hardcore function)

$$\tau_0(i,l) \stackrel{\text{def}}{=} Q^i HH^l(X)Rg(X,R)_\tau,$$

$$\rho_0 \stackrel{\text{def}}{=} \sum_{i=1}^{m}\sum_{l=1}^{n}\frac{1}{mn}|i,l\rangle\langle i,l| \otimes \tau_0(i,l).$$

4. n_0: number of qubits in ρ_0, $\quad t = \mathrm{poly}(n,\lambda)$,

$$s_Q(k) = 4n_0 t - k + O(\log(t)).$$

5. If $b = 0$, output $\mathrm{Ext}_Q(\rho_0^{\otimes t}, U_{s_Q(k)})$, where Ext_Q : quantum extractor.
6. If $b = 1$, output $U_{4n_0 t+1}$.

Proof idea

- Consider

$$\tau_0(i,l) = Q^i HH^l(X) Rg(X,R)_\tau,$$
$$\tau_1(i,l) = Q^i HH^l(X) R_\tau \otimes U_{|g(X,R)|}.$$

- To get an EFI we want:

$$\tau_0(i,l) \approx_{\mathsf{negl}_C} \tau_1(i,l),$$

$$S(\tau_1(i,l)) - S(\tau_0(i,l)) \geq \frac{1}{\mathrm{poly}(n)}.$$

- To ensure injectivity: $l \approx S(X|Q^i)_\tau$.
- To ensure $(X,H) \to Q^i HH^l(X)_\tau$ is OWSG: $l \approx S_2(X|Q^{i+1})_\tau$

$$S_2(X|Q^i)_\tau \overset{\text{def}}{=} -\log\left(\mathrm{Tr}\left((\tau^{Q^i})^{\frac{-1}{2}} \tau^{XQ^i} (\tau^{Q^i})^{\frac{-1}{2}} \tau^{XQ^i}\right)\right)$$

- Therefore need,

$$l \approx S(X|Q^i)_\tau \approx S_2(X|Q^{i+1})_\tau.$$

Proof idea

- Identify an $i^* \in [m]$

$$S(X|Q^{i^*})_\tau \approx S(X|Q^{i^*+1})_\tau$$

- **Key technical contribution**: identify a good substate γ of τ
  - $q \cdot \gamma + (1-q) \cdot \theta = \tau$
  - $q = \frac{1}{\mathrm{poly}(n)}$
  - $l_{i^*} \approx S_2(X|Q^{i^*+1})_\gamma \approx S_2(X|Q^{i^*})_\gamma \approx S(X|Q^{i^*})_\gamma$

- Consider
  - $\sigma_0 \stackrel{\mathrm{def}}{=} Q^{i^*} HH^{l_{i^*}}(X) Rg(X,R)_\gamma$
  - $\sigma_1 \stackrel{\mathrm{def}}{=} Q^{i^*} HH^{l_{i^*}}(X) R_\gamma \otimes U_{|g(X,R)|}$
  - since $l_{i^*} \approx S(X|Q^{i^*})_\gamma$: $\quad S(\sigma_1) - S(\sigma_0) \geq O(\log n)$
  - since $l_{i^*} \approx S_2(X|Q^{i^*+1})_\gamma$: $\quad \sigma_1 \approx_{\mathsf{negl}_c} \sigma_0$

Proof idea

- Consider

$$\begin{aligned}\tau_0(i^*, l_{i^*}) &\stackrel{\text{def}}{=} Q^{i^*} HH^{l_{i^*}}(X) Rg(X,R)_\tau \\ &= q \cdot \sigma_0 + (1-q) \cdot Q^{i^*} HH^{l_{i^*}}(X) Rg(X,R)_\theta \\ \tilde{\tau}_1(i^*, l_{i^*}) &\stackrel{\text{def}}{=} q \cdot \sigma_1 + (1-q) \cdot Q^{i^*} HH^{l_{i^*}}(X) Rg(X,R)_\theta\end{aligned}$$

- Since $q \geq \frac{1}{\mathrm{poly}(n)}$: $\quad S(\tilde{\tau}_1(i^*, l_{i^*})) - S(\tau_0(i^*, l_{i^*})) \geq \frac{1}{\mathrm{poly}(n)}$
- Since $\sigma_1 \approx_{\mathsf{negl}_C} \sigma_0$: $\quad \tilde{\tau}_1(i^*, l_{i^*}) \approx_{\mathsf{negl}_C} \tau_0(i^*, l_{i^*})$

Proof idea

- Since i^* and l_{i^*} cannot be efficiently determined, take a convex mixture:

$$\rho_0 \stackrel{\text{def}}{=} \sum_{i=1}^{m} \sum_{l=1}^{n} \frac{1}{mn} |i, l\rangle\langle i, l| \otimes \tau_0(i, l)$$

$$\rho_1 \stackrel{\text{def}}{=} \sum_{i=1}^{m} \sum_{l=1}^{n} \mathbb{1}(i \neq i^* \text{ or } l \neq l_{i^*}) \cdot \frac{1}{mn} |i, l\rangle\langle i, l| \otimes \tau_0(i, l) + \frac{1}{mn} |i^*, l_{i^*}\rangle\langle i^*, l_{i^*}| \otimes \tilde{\tau}_1(i^*, l_{i^*})$$

Proof idea

- Since $S(\tilde{\tau}_1(i^*, l_{i^*})) - S(\tau_0(i^*, l_{i^*})) \geq \frac{1}{\mathrm{poly}(n)}$

$$S(\rho_1) - S(\rho_0) \geq \frac{1}{\mathrm{poly}(n)}$$

- Since $\tilde{\tau}_1(i^*, l_{i^*}) \approx_{\mathsf{negl}_C} \tau_0(i^*, l_{i^*})$: $\quad \rho_1 \approx_{\mathsf{negl}_C} \rho_0$
- Take t $(\in \mathrm{poly}(n))$ copies $\rho_0^{\otimes t}, \rho_1^{\otimes t}$
  - $S_0(\rho_0^{\otimes t}) \rightarrow t \cdot S(\rho_0)$; $S_1(\rho_1^{\otimes t}) \rightarrow t \cdot S(\rho_1)$
  - $S_1(\rho_1^{\otimes t}) >> S_0(\rho_0^{\otimes t})$
  - $\rho_1^{\otimes t} \approx_{\mathsf{negl}_C} \rho_0^{\otimes t}$
- Ext_Q removes non-uniformity in $\rho_1^{\otimes t}$ $(k^* \stackrel{\mathrm{def}}{=} S_1(\rho_1^{\otimes t}))$
  - $k \leq k^*$: $\mathsf{Ext}_Q(\rho_0^{\otimes t}, U_{s_Q(k^*)}) \approx_{\mathsf{negl}_C} \mathsf{Ext}_Q(\rho_1^{\otimes t}, U_{s_Q(k^*)}) \approx_{\mathsf{negl}_C} U_{4n_0t+1}$
  - $k \geq k^*$: $\mathsf{Ext}_Q(\rho_0^{\otimes t}, U_{s_Q(k^*)})$ is far from U_{4n_0t+1}

Identifying γ: Flattening

- Consider the spectral decomposition:

$$\tau^{XQ^{i^*}} = \sum_{x,k} p_{x,k} |x\rangle\langle x|^X \otimes |e_{x,k}\rangle\langle e_{x,k}|^{Q^{i^*}}.$$

- Consider a function J
  - $J(p_{x,k}) = r$ if $p_{x,k} \in \left(\frac{1}{2^r}, \frac{1}{2^{r-1}}\right]$ for $r \in [\mathrm{poly}(n)]$,
  - $J(p_{x,k}) = 0$ otherwise.

- Consider the extension:

$$\tau^{XQ^{i^*}J} \stackrel{\mathrm{def}}{=} \sum_{x,k} p_{x,k} |x\rangle\langle x|^X \otimes |e_{x,k}\rangle\langle e_{x,k}|^{Q^{i^*}} \otimes |J(p_{x,k})\rangle\langle J(p_{x,k})|^J.$$

- Conditioned on any non-zero $J = j$: $\tau_j^{XQ^{i^*}}$ is nearly "flat".

Identifying γ: Flattening

- Consider the conjugation

$$\theta^{XQ^{i^*}} = (\tau^{Q^{i^*}})^{\frac{-1}{2}} \tau^{XQ^{i^*}} (\tau^{Q^{i^*}})^{\frac{-1}{2}}.$$

- Add the J register according to the eigenvalues to get $\theta^{XQ^{i^*}J}$.
- Conjugate back

$$\tau^{XQ^{i^*}J} = (\tau^{Q^{i^*}})^{\frac{1}{2}} \theta^{XQ^{i^*}J} (\tau^{Q^{i^*}})^{\frac{1}{2}}.$$

- Conditioned on any non-zero $J = j$:

$$S_2(X|Q^{i^*})_{\tau_j^{XQ^{i*}}} \approx S(X|Q^{i^*})_{\tau_j^{XQ^{i*}}}.$$

- Need $S_2(X|Q^{i^*+1})_\gamma \approx S_2(X|Q^{i^*})_\gamma \approx S(X|Q^{i^*})_\gamma$.
- Identify γ as an appropriate substate of $\tau_j^{XQ^{i^*}}$ for some j.

EFI $\implies$ sv-OWSG

sv-OWSG(1^λ)

1. Input: the security parameter λ.
2. Subroutine: EFI-pair generator (ρ_0, ρ_1).
3. $\textsc{KeyGen}(1^\lambda)$: $x \leftarrow U_n$ for $n = \lambda$.
4. $\textsc{StateGen}(1^\lambda, x)$: $\phi_x = \rho_{x_1} \otimes \rho_{x_2} \cdots \otimes \rho_{x_n}$ where x_i represents the i^{th}-bit of x.
5. $\textsc{Ver}(x', \phi_x)$
   - let $\{\pi_0, \pi_1\}$ be an optimal distinguisher for ρ_0 and ρ_1.
   - $\textsc{Ver}$ measures ϕ_x according to the projectors $\{\pi_{x_1'} \otimes \pi_{x_2'} \cdots \otimes \pi_{x_n'}, \mathbb{I} - \pi_{x_1'} \otimes \pi_{x_2'} \cdots \otimes \pi_{x_n'}\}$.
   - outputs $\top$ if the first result is obtained and outputs $\perp$ otherwise.

Proof idea: $\mathrm{EFI} \implies$ sv-OWSG

- $\|\rho_0 - \rho_1\|_1 \geq 1 - \mathsf{negl}(\lambda)$ ensures

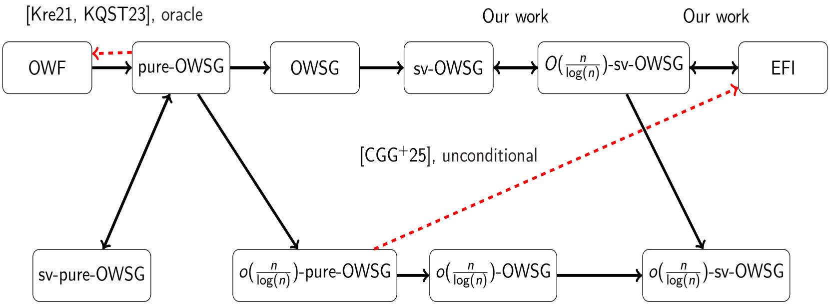
$$\Pr(\top \leftarrow \textsc{Ver}(x, \phi_x)) \geq 1 - \mathsf{negl}(\lambda).$$

- $\rho_0 \approx_{\mathsf{negl}_C} \rho_1$ ensures non-invertibility by QPT adversary $\mathcal{A}$
  - $\mathcal{A}$ must output $x' = x$
  - this can be used to distinguish ρ_0 and ρ_1 by inserting at a random i and calling $\mathcal{A}$

Summary

- Show $O\left(\frac{n}{\log(n)}\right)$-copy sv-$\mathrm{OWSG}$s are equivalent to EFI (and quantum commitments).
- Implies construction of commitments from a mixed-state output OWSG.
- Provide an alternative to the construction provided by [HILL99] to obtain a PRG from OWF.

Open Questions



- Can we get expanding 1-PRS (quantum equivalent of PRG) from OWSG?

References I

Prabhanjan Ananth, Luowen Qian, and Henry Yuen.
Cryptography from Pseudorandom Quantum States.
In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 208–236, Cham, 2022. Springer Nature Switzerland.

James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma.
One-Way Functions Imply Secure Computation in a Quantum World.
In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 467–496, Cham, 2021. Springer International Publishing.

Zvika Brakerski, Ran Canetti, and Luowen Qian.
On the Computational Hardness Needed for Quantum Cryptography.
In *14th Innovations in Theoretical Computer Science Conference (ITCS)*, 2023.

Bruno Cavalar, Eli Goldin, Matthew Gray, Peter Hall, Yanyi Liu, and Angelos Pelecanos.
On the Computational Hardness of Quantum One-Wayness.
Quantum, 9:1679, March 2025.

Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan.
Oblivious Transfer Is in MiniQCrypt.
In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 531–561, Cham, 2021. Springer International Publishing.

Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby.
A Pseudorandom Generator from any One-way Function.
SIAM Journal on Computing, 1999.

William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal.
Quantum Cryptography in Algorithmica.
In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC, 2023.

References II

William Kretschmer.
Quantum Pseudorandomness and Classical Complexity.
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

Dakshita Khurana and Kabir Tomer.
Commitments from Quantum One-Wayness.
ACM Symposium on Theory of Computing (STOC), 2024.

Tomoyuki Morimae and Takashi Yamakawa.
Quantum commitments and signatures without one-way functions.
In *Advances in Cryptology – CRYPTO*, 2022.

Jun Yan.
General Properties of Quantum Bit Commitments.
In *Advances in Cryptology – ASIACRYPT*, 2022.

Thanks!