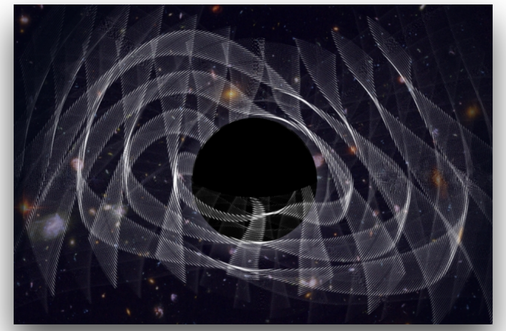
A Combinatorial Approach to Quantum Random Function

Nico Döttling Giulio Malavolta Sihang Pu

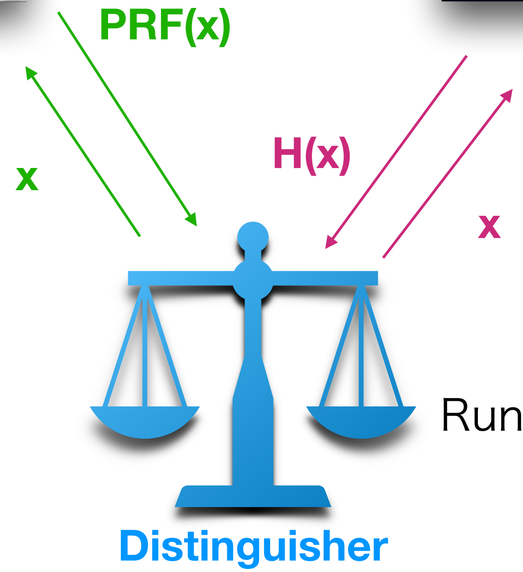
Overview

- Background and motivations
- Challenges
- Results
- Construction
- Conclusion

Pseudorandom Functions



This PRF has to be computed efficiently



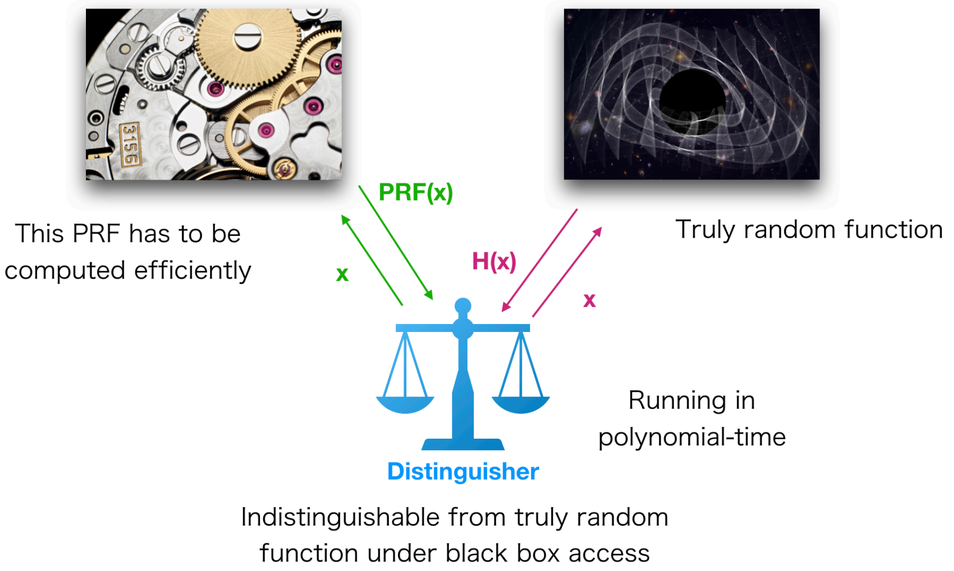
Truly random function

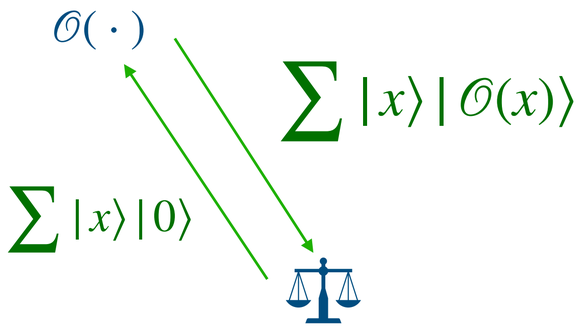
Running in polynomial-time

Indistinguishable from truly random function under black box access

PRF in quantum world

- PRF analogues in quantum world (two definitions)
  - Post-quantum PRF:
    - quantum security for classical queries
  - Quantum-secure PRF (QPRF):
    - the distinguisher can send quantum queries





Applications of QPRF

- Quantum money
  - Backed by no-cloning theorem thus impossible to forge
  - Intrinsically ideal for banknotes
- Pseudorandom quantum states
- Quantum secure MACs

Related works

- We focus on quantum-secure PRF (even if quantum queries are allowed) in this work
- Zhandry investigated these notions heavily (eg. FOCS'12, CRYPTO'12)
  - Separation result: if secure PRFs exist, then there are standard-secure (post-quantum) PRFs that are not QPRFs.

Motivation

- Zhandry gave the separation result and proved that many constructions of post-quantum PRFs are also quantum-secure, though with completely different analysis.
  - These proofs are complicated and not tight
- Our goal: A generic construction, a simple analysis, and a tight proof?
- Inspiration: domain extension techniques
- Challenge: it's not trivial to extend the domain (even for truly random functions)

Challenge

- It is challenging to extend truly random function's domain
- Suppose we have a truly random function $f : \{0,1\}^{\lambda} \to \{0,1\}^{\lambda}$
- We would like to extend it by using a random linear function (or universal hash function) $H : \{0,1\}^{2\lambda} \to \{0,1\}^{\lambda}$ in this way:
  - $f' : x \to f(H(x))$

Challenge (cont.)

- This is statistically indistinguishable from a truly random function for classical distinguisher with oracle access
- However, Boneh and Lipton in [BL95] suggested that via superposition queries, one can find the period of a function efficiently
- In this case, one can find the kernel of our linear function $H(\cdot)$ thus makes f' distinguishable

Results

- Explore a different road to construct QPRF which is based on the framework of Döttling and Schröder in CRYPTO'15 and have the following result:
  - Given any post-quantum PRF with small-domain, our construction extends it to a full-fledged QPRF
- The key ingredient is a highly unbalanced bipartite expander [GUV09]
  - It crucially allows us to reduce the quantum hardness of our PRF to the classical (post-quantum) hardness of a small-domain PRF

Results (cont.)

- Our construction preserves the key-homomorphic property of underlying PRF, giving a quantum key-homomorphic PRF for free

- Key-homomorphic PRFs were introduced by Boneh et al. In a nutshell, for key-homomorphic PRFs the key-space is a group and it holds for all x that
  $\mathrm{PRF}(K_1 + K_2, x) = \mathrm{PRF}(K_1, x) + \mathrm{PRF}(K_2, x)$.

- Key-homomorphic PRFs have applications in the context of proxy-re-encryption and related key security.

- It give rise to a very natural protocol for a distributed PRF

Outline

- There are two steps, a domain extension step and a combiner step
- The domain extension step takes a small domain PRF with domain size *poly(q)* and constructs from it a *q*-bounded PRF on a large domain.
  - A PRF is called *q*-bounded if security is only guaranteed for adversaries which make at most *q* queries.
- The combiner step, combines a small number of bounded PRFs which have the same domain.

Combiner Step

- The key idea here is to set the bounds in an exponentially increasing way.

- Specifically, if $\mathsf{F}_q(K_q, x)$ are q-bounded PRFs, we combine them into a function F via

- $F(K, x) = \bigoplus_{i=1}^{t} \mathsf{F}_{2^i}(K_{2^i}, x)$, where $K = (K_{2^1}, \ldots, K_{2^t})$, where t will be chosen slightly super-logarithmic in the security parameter λ.

Combiner Step (cont.)

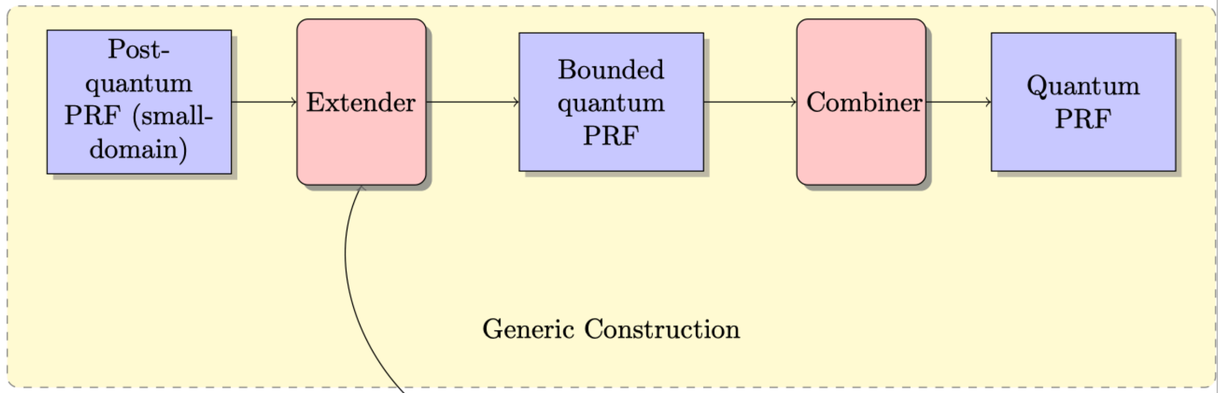
- We claim that if $\mathsf{F}_q(K_q, x)$ is a q-bounded QPRF as long as q is polynomial, then $F(K, x)$ is an unbounded QPRF.

- The security derives from the following fact: for an efficient (BQP) distinguisher, there is an upper bound q' on the number of superposition queries it can make. Thus we are able to choose $i' = \lceil \log q' \rceil \leq t$ to reduce the security of F to the i'-th bounded PRF $\mathsf{F}_{2^{i'}}$.

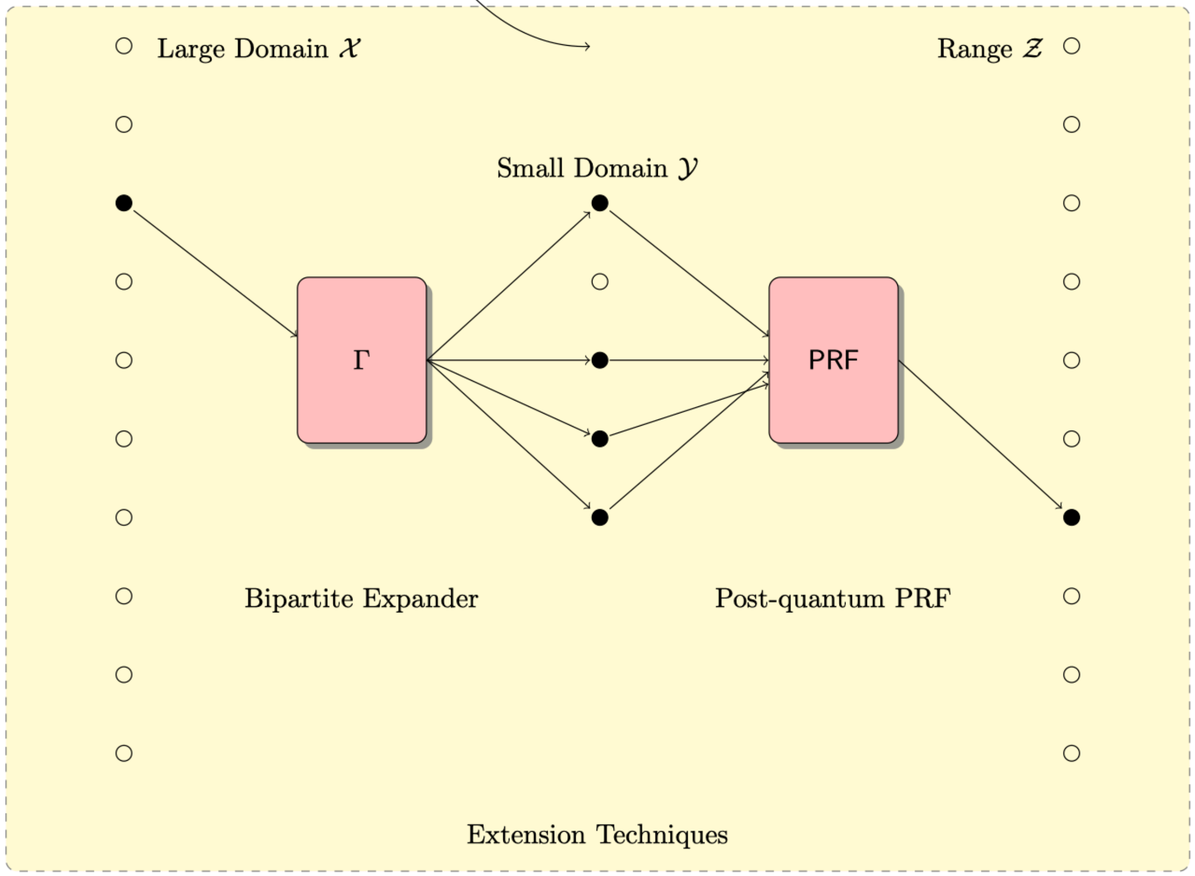
Domain Extension Step

- As mentioned, domain extension is challenging
- As shown before, statistically secure against classical adversary is not sufficient
- We need a perfectly secure domain extension step
- If so, we can use the Zhandry's lemma [FOCS'12] which states that any classical $2q$-wise-independent function is identically distributed to a uniform function from the view of a q-bounded quantum adversary.

Perfectly secure domain extension from highly unbalanced bipartite expander



A bipartite graph Γ where the set of left vertices $[N]$ can be made super-polynomially large, the set of right vertices $[L]$ is only polynomially large and the degree D is poly-logarithmic.

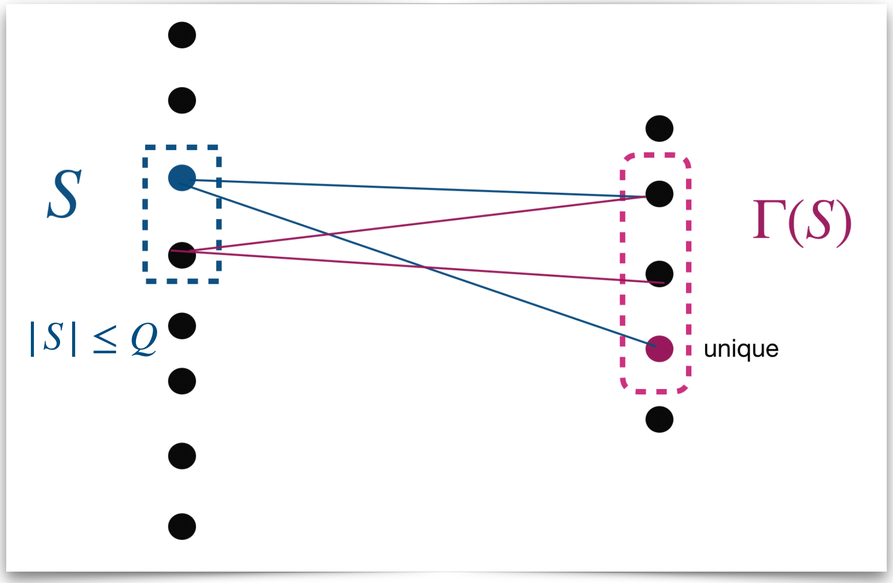


Q-unique

- Moreover, we require an additional unique neighbour property for unbalanced bipartite expander:

- For any subset $S \subset [N]$ of left-vertices not larger than a (polynomial) bound Q, there exists a vertex v in $\Gamma(S) \subset [L]$ (the neighbourhood of S) which has a unique neighbour in S.

  - A construction of such graph is given in [GUV09]



Extend a random function

- First, we show how to extend a small-domain truly random function to Q-wise-independent function (where Q will be selected later)
  - Q-wise-independent: for any pairwise distinct $x_1, \ldots, x_Q \in [N]]$ that $g(x_1), \ldots, g(x_Q)$ are independent and uniformly random
- With a Q-unique expander Γ, for a random function f defined on the small domain $[L]$, we extend it to a Q-wise-independent function g defined on the large domain $[N]$:
  - $g(x) = \oplus_{j \in [D]} f(\Gamma(x, j))$, where $\Gamma(x, j)$ is the j-th neighbour of x.

Sketch of the Proof$_1$

- By the Q-unique property of Γ, for any subset $S' \subset S = \{x_1, \ldots, x_Q\}$, there exist a vertex $v' \in \Gamma(S')$ having a unique neighbour $x_{i'} \in S'$
- Thus there is an index $j' \in [D]$ such that $f(\Gamma(x_{i'}, j'))$ only appears in $g(x_{i'})$ but not other $g(x_i)$
- Given $f(\Gamma(x_{i'}, j')$ is uniformly random and independent of other $g(x_i)$, so is $g(x_{i'})$
- Therefore we can recursively repeat to show every $g(x_i)$ is uniformly random and independent

Replace it with a PRF

- Then, we replace the random function with a small-domain PRF and choose $Q = 2q$.
- We claim that if it is a post-quantum PRF with (polynomially-sized) domain $[L]$, then it holds that
  - $F(K, x) = \bigoplus_{j \in [D]} \mathrm{PRF}(K, \Gamma(x, j))$ is indistinguishable from the $2q$-wise-independent function $g(x) = \bigoplus_j f(\Gamma(x, j))$ for a q-bounded BQP quantum adversary
- Finally, by using Zhandry's lemma, it directly implies the $2q$-uniform function $F(K, x)$ is indeed a q-bounded QPRF

Sketch of the Proof$_2$

- Suppose a q-bounded BQP adversary $\mathcal{A}$ can distinguish between $F(K, x)$ and $g(x)$, we will show another $\mathcal{A}'$ can break the post-quantum security of underlying PRF

- Let the adversary $\mathcal{A}'$ classically query the oracle $\mathcal{O}$ (on a small-domain) to build its function table, then locally computes a quantum circuit $U_{\mathcal{O}}$ such that $U_{\mathcal{O}}|x, y\rangle = |x, y + \mathcal{O}(x)\rangle$

- Now, $\mathcal{A}'$ gives $\mathcal{A}$ superposition access to its simulated oracle $\mathcal{O}' : |x, y\rangle \rightarrow U_{\mathcal{O}}|x, y\rangle$ and outputs what $\mathcal{A}$ outputs

- Clearly, if $\mathcal{A}$ can distinguish $F(K, x)$ from $g(x)$, then $\mathcal{A}'$ can distinguish PRF from a truly random function

Summary

- Generic and simple construction
- No need to go through GGM construction
- Optimally tight proof

Thank you!