Pasqal Defining the quantum reality

Lecture 5: Shor's algorithm

January 28, 2026

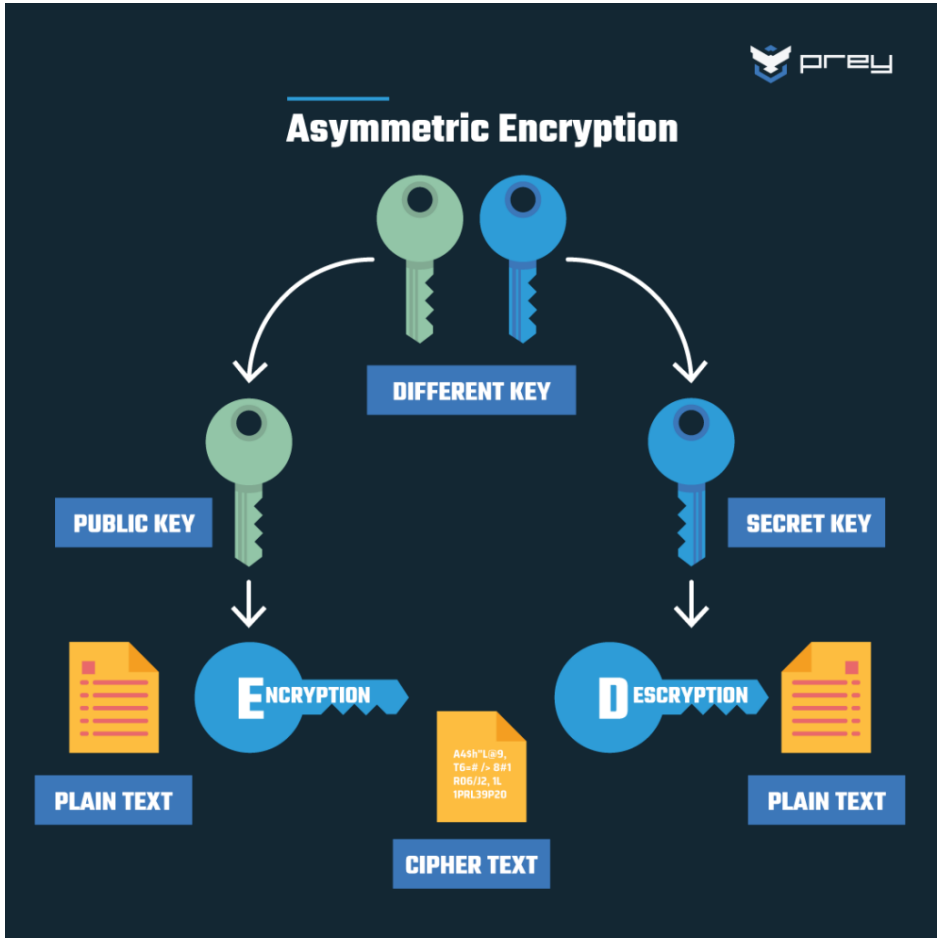
Known algorithms with exponential speedup

Pasqal

Name	G	X	K	Function
Deutsch	$\{0,1\}, \oplus$	$\{0,1\}$	$\{0\}$ or $\{0,1\}$	$K=\{0,1\}: \begin{cases} f(x)=0 \\ f(x)=1 \end{cases}$ $K=\{0\}: \begin{cases} f(x)=x \\ f(x)=1-x \end{cases}$
Simon	$\{0,1\}^n, \oplus$	any finite set	$\{0,s\}$ $s \in \{0,1\}^n$	$f(x \oplus s) = f(x)$
Period-finding	$\mathbf{Z}, +$	any finite set	$\{0,r,2r,\ldots\}$ $r \in G$	$f(x+r) = f(x)$
Order-finding	$\mathbf{Z}, +$	$\{a^j\}$ $j \in Z_r$ $a^r = 1$	$\{0,r,2r,\ldots\}$ $r \in G$	$f(x) = a^x$ $f(x+r) = f(x)$
Discrete logarithm	$\mathbf{Z}_r \times \mathbf{Z}_r$ + (mod r)	$\{a^j\}$ $j \in Z_r$ $a^r = 1$	$(\ell, -\ell s)$ $\ell, s \in \mathbf{Z}_r$	$f(x_1,x_2) = a^{kx_1+x_2}$ $f(x_1+\ell, x_2-\ell s) = f(x_1,x_2)$
Order of a permutation	$\mathbf{Z}_{2^m} \times \mathbf{Z}_{2^n}$ + (mod 2^m)	$\mathbf{Z}_{2^n}$	$\{0,r,2r,\ldots\}$ $r \in X$	$f(x,y) = \pi^x(y)$ $f(x+r,y) = f(x,y)$ π = permutation on X
Hidden linear function	$\mathbf{Z} \times \mathbf{Z}, +$	$\mathbf{Z}_N$	$(\ell, -\ell s)$ $\ell, s \in X$	$f(x_1,x_2) =$ $\pi(sx_1 + x_2 \bmod N)$ π = permutation on X
Abelian stabilizer	(H,X) H = any Abelian group	any finite set	$\{s \in H \mid f(s,x) = x, \forall x \in X\}$	$f(gh,x) = f(g,f(h,x))$ $f(gs,x) = f(g,x)$

Cryptography using RSA

Pasqal



RSA Algorithm

Key Generation

Select p,q	p and q both prime; $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e,n\}$
Private key	$KR = \{d,n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Plaintext:	C
Ciphertext:	$M = C^d \pmod n$

How to factor 2048 bit RSA integers with less than a million noisy qubits

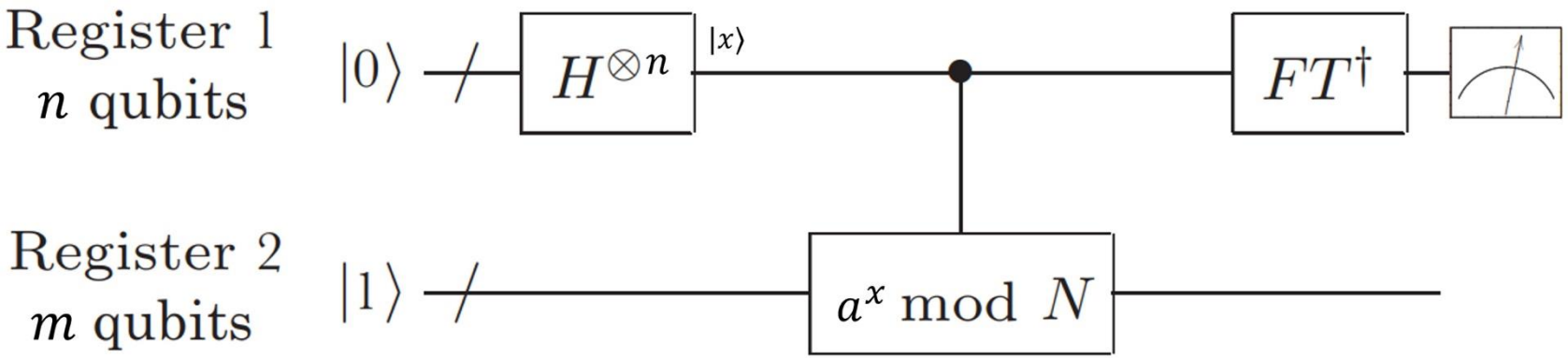
Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA

June 9, 2025

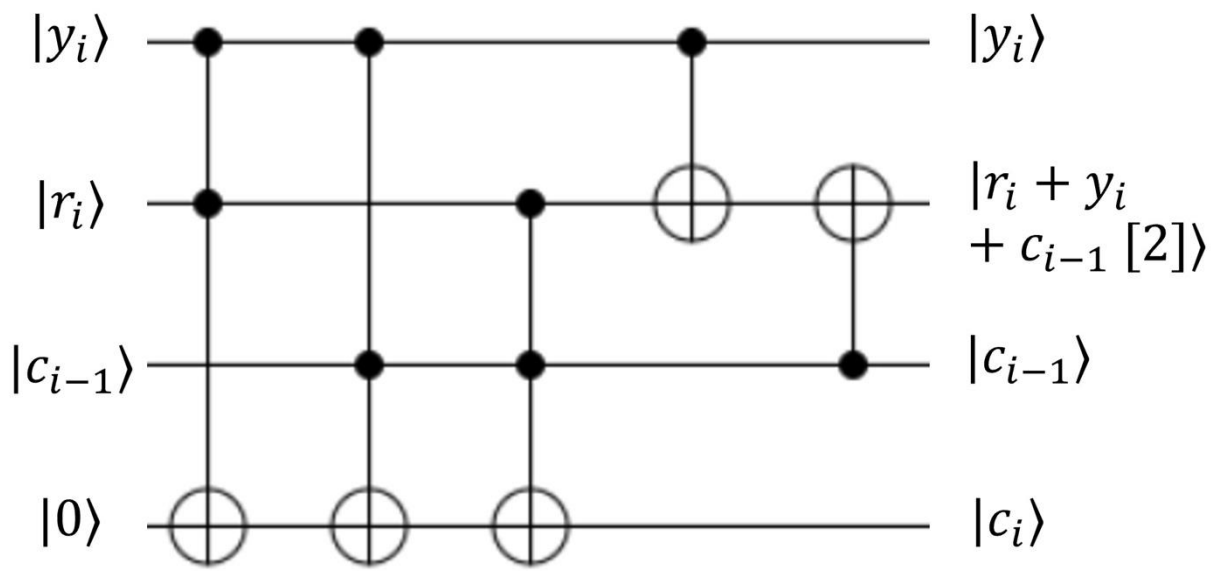
Quantum part of Shor

Pasqal



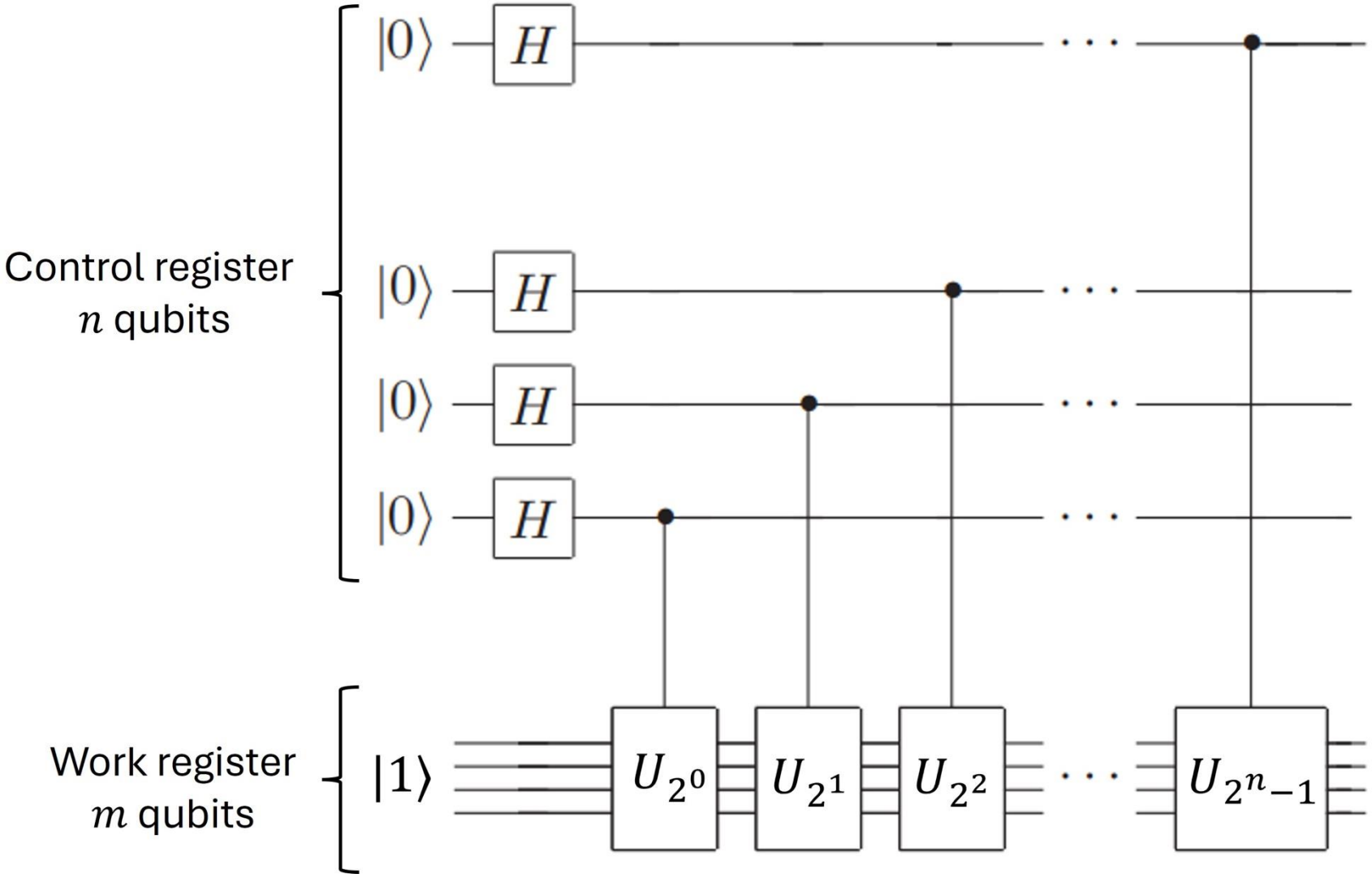
Adder

Pasqal



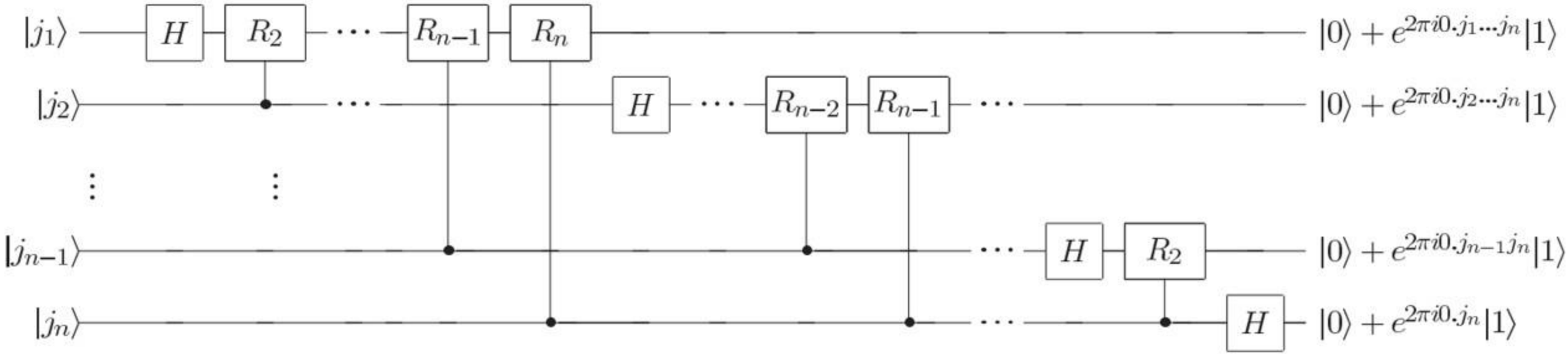
Modular exponentiation

Pasqal



QFT

Pasqal


$|j_1\rangle$
$|j_2\rangle$
$|j_{n-1}\rangle$
$|j_n\rangle$
H
R_2
R_{n-1}
R_n
H
R_{n-2}
R_{n-1}
H
R_2
H
$|0\rangle + e^{2\pi i 0.j_1 \cdots j_n}|1\rangle$
$|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle$
$|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle$
$|0\rangle + e^{2\pi i 0.j_n}|1\rangle$