Quantum algorithms for computing short discrete logarithms and factoring RSA integers

Martin Ekerå[1,2] Johan Håstad[1]

[1] KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden

[2] Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

PQCrypto 2017, 8th International Workshop, Utrecht, June 26-28, 2017

SWEDISH ARMED FORCES

Introduction

Our contribution

- We modify Shor's algorithms to more efficiently solve
  - the *short* discrete logarithm problem
  - the *RSA* integer factoring problem

- The main hurdle is to exponentiate group elements. We shorten the exponents.

The integer factoring problem

The integer factoring problem (IFP)

- Given an integer N compute its prime factors.

The integer factoring problem

The integer factoring problem (IFP)

- Given an integer N compute its prime factors.

The RSA integer factoring problem (RSA IFP)

- $N = pq$ where p and $q \neq p$ are two large primes of similar size

The integer factoring problem

The integer factoring problem (IFP)

- Given an integer N compute its prime factors.

The RSA integer factoring problem (RSA IFP)

- $N = pq$ where p and $q \neq p$ are two large primes of similar size

- We focus on the RSA IFP since it is of cryptographic significance.

The discrete logarithm problem

The discrete logarithm problem (DLP)

- Given a generator g of some group $\mathbb{G}$ and $x = g^d$ compute $d = \log_g x$.

The discrete logarithm problem

The discrete logarithm problem (DLP)

- Given a generator g of some group $\mathbb{G}$ and $x = g^d$ compute $d = \log_g x$.

The short discrete logarithm problem (short DLP)

- $d \lll r$ where r is the order of $\mathbb{G}$
- r may be assumed known or unknown

Reasons for studying the short DLP

Reasons for studying the short DLP

1. The RSA IFP may be reduced to the short DLP.
2. The short DLP arises in some parameterizations of DLP-based schemes.

Reducing RSA IFP to a short DLP [HSS93]

1. Let $N = pq$ be the RSA integer to be factored.
2. Pick a random $g \in \mathbb{Z}_N^*$. Compute
$$x = g^N \equiv g^{p+q-1} \quad \text{since the order of } \mathbb{Z}_N^* \text{ is} \quad pq - p - q + 1.$$
3. Compute $d = p + q - 1$ given g and x.
4. Solve $N = pq$ and $d = p + q - 1$ for p and q.

- An RSA IFP may be reduced to a short DLP in a group of unknown order.

Domain parameters for DLP-based schemes

Group	Prime p	Order r	Exponent d	Classical security
Elliptic curve $E(\mathbb{F}_p)$	200	200	200	100
Safe-prime $\mathbb{G} \subset \mathbb{F}_p^*$	2048	2047	2047	* 100
— short d	2048	2047	200	* 100
Schnorr $\mathbb{G} \subset \mathbb{F}_p^*$	2048	200	200	* 100

* ballpark figure — various models exist for estimating these security levels

- The short DLP arises when short exponents are used with safe-prime groups.
- Important to understand quantum implications of parameterization choices.

Shor's algorithms [Shor94]

Shor's algorithms

- Shor's algorithms solve the IFP and the DLP in $\mathbb{F}_p^*$.
- May be generalized to solve the DLP in any finite cyclic group.

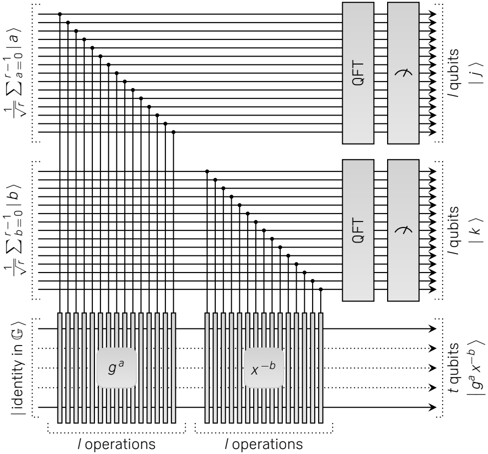
Shor's algorithm for the DLP [Shor94]

1. Compute the superposition

$$\frac{1}{r}\sum_{a=0}^{r-1}\sum_{b=0}^{r-1}\left|\,a,\,b,\,g^{a}\,x^{-b}\,\right\rangle$$

   where $\langle\, g\,\rangle = \mathbb{G}$ of order $r \sim 2^l$.

2. Compute two QFTs of size r.
3. Observe frequencies j and k.
4. Solve $dj + k \equiv 0 \pmod{r}$.



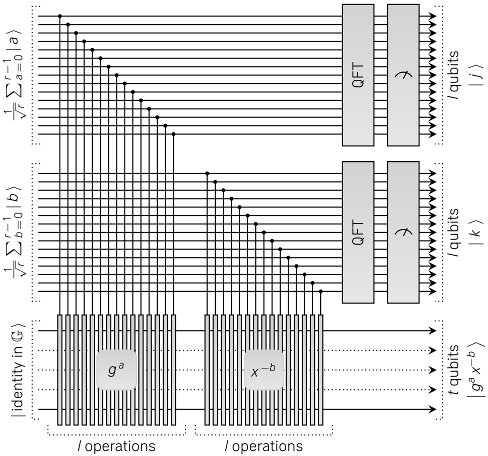
Shor's algorithm for the DLP [Shor94]

1. Compute the superposition

   $$\frac{1}{r}\sum_{a=0}^{r-1}\sum_{b=0}^{r-1}\left|a,\, b,\, g^{a}x^{-b} \equiv g^{(a-bd) \bmod r}\right\rangle$$

   where $\langle g \rangle = \mathbb{G}$ of order $r \sim 2^{l}$.

2. Compute two QFTs of size r.
3. Observe frequencies j and k.
4. Solve $dj + k \equiv 0 \pmod{r}$.



Shor's algorithm for the DLP [Shor94]

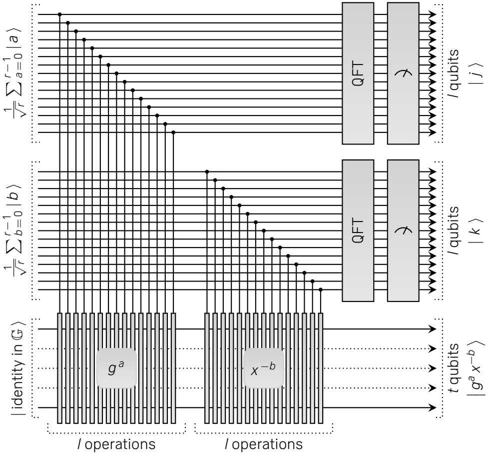
1. Compute the superposition

$$\frac{1}{r}\sum_{a=0}^{r-1}\sum_{b=0}^{r-1}\left|\, a,\, b,\, g^{a}x^{-b} \equiv g^{(a-bd) \bmod r}\right\rangle$$

   where $\langle g \rangle = \mathbb{G}$ of order $r \sim 2^l$.

2. Compute two QFTs of size 2^l.
3. Observe frequencies j and k.
4. Solving for d yields

$$d \equiv \left\lfloor \frac{kr}{2^l} \right\rceil z^{-1} \pmod r \quad \text{where} \quad z = \frac{\{jr\}_{2^l} - jr}{2^l} \in \mathbb{Z}.$$



Shor's algorithm for the DLP [Shor94]

Group	Prime p	Order r	Exponent d	Classical security
Elliptic curve $E(\mathbb{F}_p)$	200	200	200	100
Safe-prime $\mathbb{G} \subset \mathbb{F}_p^*$	2048	2047	2047	* 100
— short d	2048	2047	200	* 100
Schnorr $\mathbb{G} \subset \mathbb{F}_p^*$	2048	200	200	* 100

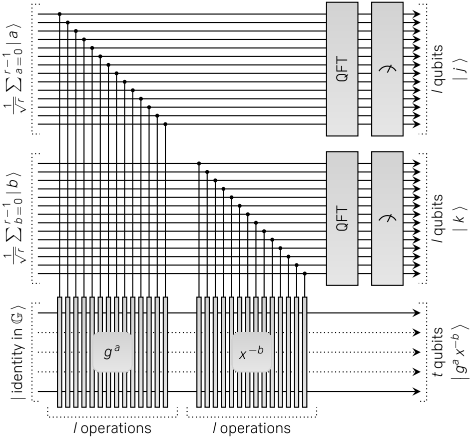
1. Compute the superposition

$$\frac{1}{r} \sum_{a=0}^{r-1} \sum_{b=0}^{r-1} \left| a,\, b,\, g^{a} x^{-b} \equiv g^{(a-bd) \bmod r} \right\rangle$$

   where $\langle g \rangle = \mathbb{G}$ of order $r \sim 2^l$.

2. Compute two QFTs of size 2^l.
3. Observe frequencies j and k.
4. Solving for d yields

$$d \equiv \left\lfloor \frac{kr}{2^l} \right\rceil z^{-1} \pmod r \quad \text{where} \quad z = \frac{\{jr\}_{2^l} - jr}{2^l} \in \mathbb{Z}.$$



Shor's algorithm for the DLP [Shor94]

1. Compute the superposition

$$\frac{1}{r}\sum_{a=0}^{r-1}\sum_{b=0}^{r-1}\left|\,a,\, b,\, g^{a}x^{-b} \equiv g^{(a-bd) \bmod r}\right\rangle$$

where $\langle\, g\,\rangle = \mathbb{G}$ of order $r \sim 2^{l}$.

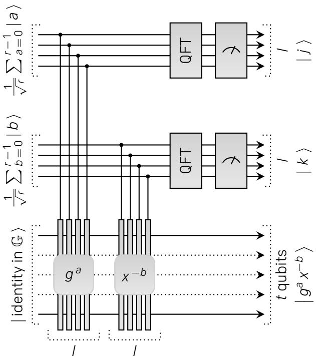
2. Compute two QFTs of size 2^{l}.

3. Observe frequencies j and k.

4. Solving for d yields

$$d \equiv \left\lfloor \frac{kr}{2^{l}} \right\rceil z^{-1} \pmod{r} \quad \text{where} \quad z = \frac{\{jr\}_{2^{l}} - jr}{2^{l}} \in \mathbb{Z}.$$

Group	Prime p	Order r	Exponent d	Classical security
Elliptic curve $E(\mathbb{F}_p)$	200	200	200	100
Safe-prime $\mathbb{G} \subset \mathbb{F}_p^*$	2048	2047	2047	* 100
— short d	2048	2047	200	* 100
Schnorr $\mathbb{G} \subset \mathbb{F}_p^*$	2048	200	200	* 100



Shor's algorithm for the DLP [Shor94]

Group	Prime p	Order r	Exponent d	Classical security
Elliptic curve $E(\mathbb{F}_p)$	200	200	200	100
Safe-prime $\mathbb{G} \subset \mathbb{F}_p^*$	2048	2047	2047	* 100
— short d	2048	2047	200	* 100
Schnorr $\mathbb{G} \subset \mathbb{F}_p^*$	2048	200	200	* 100

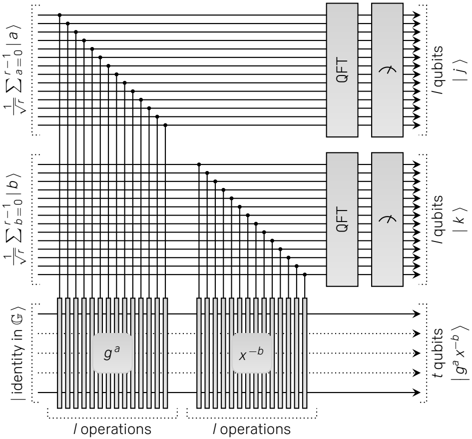
1. Compute the superposition

$$\frac{1}{r} \sum_{a=0}^{r-1} \sum_{b=0}^{r-1} \left| a,\, b,\, g^a x^{-b} \equiv g^{(a-bd) \bmod r} \right\rangle$$

where $\langle g \rangle = \mathbb{G}$ of order $r \sim 2^l$.

2. Compute two QFTs of size 2^l.
3. Observe frequencies j and k.
4. Solving for d yields

$$d \equiv \left\lfloor \frac{kr}{2^l} \right\rceil z^{-1} \pmod{r} \quad \text{where} \quad z = \frac{\{jr\}_{2^l} - jr}{2^l} \in \mathbb{Z}.$$



Our algorithm for the short DLP

Our improvements

1. We make the exponent length depend on d.
2. We enable tradeoffs between the exponent length and the number of runs.

- This parallels Seifert's modification [Seifert01] of Shor's order finding algorithm.

- We provide a full analysis of the algorithm and rigorous proofs.

Our algorithm for the short DLP [Ekerå16] — *single pair*

1. Compute the superposition

$$\frac{1}{\sqrt{2^{3m}}} \sum_{a=0}^{2^{2m}-1} \sum_{b=0}^{2^m-1} |\, a,\, b,\, g^a x^{-b} = g^{a-bd} \,\rangle$$

where $\langle\, g \,\rangle = \mathbb{G}$ of order r and $d < 2^m \lll r$.

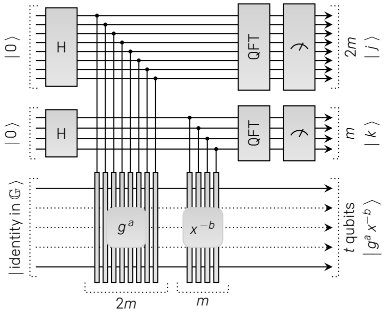
2. Compute QFTs of size 2^{2m} and 2^m.

3. Observe frequencies j and k.

4. Solve $|\, \{dj + 2^m k\}_{2^{2m}} \,| \leq 2^{m-2}$ for d.

   The probability of a good pair is $\geq 1/8$.
   Need a single good pair to solve for d.
   The order r may be unknown.

Group	Prime p	Order r	Exponent d	Classical security
Elliptic curve $E(\mathbb{F}_p)$	200	200	200	100
Safe-prime $\mathbb{G} \subset \mathbb{F}_p^*$	2048	2047	2047	* 100
— short d	2048	2047	200	* 100
Schnorr $\mathbb{G} \subset \mathbb{F}_p^*$	2048	200	200	* 100



Our algorithm for the short DLP — *multiple pairs*

1. Compute the superposition

$$\frac{1}{\sqrt{2^{2\ell+m}}} \sum_{a=0}^{2^{\ell+m}-1} \sum_{b=0}^{2^{\ell}-1} \left| a,\, b,\, g^{a} x^{-b} = g^{a-bd} \right\rangle$$

where $d < 2^m \lll r$ and $\ell \approx m/s$ for small s.

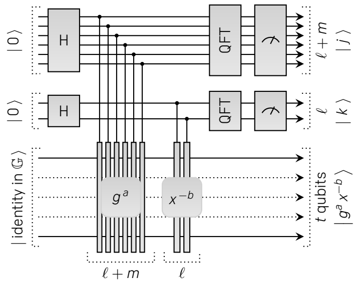
2. Compute QFTs of size $2^{\ell+m}$ and 2^{ℓ}.

3. Observe frequencies j and k.

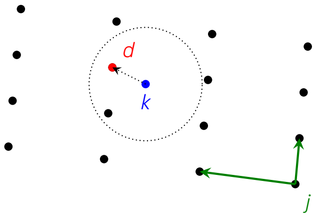
Expect $\left| \{dj + 2^m k\}_{2^{\ell+m}} \right| \leq 2^{m-2}$.

The probability of a good pair is $\geq 1/8$.
Need at least s good pairs to solve for d.
The order r may be unknown.

Group	Prime p	Order r	Exponent d	Classical security
Elliptic curve $E(\mathbb{F}_p)$	200	200	200	100
Safe-prime $\mathbb{G} \subset \mathbb{F}_p^*$	2048	2047	2047	* 100
— short d	2048	2047	200	* 100
Schnorr $\mathbb{G} \subset \mathbb{F}_p^*$	2048	200	200	* 100



Classical post-processing



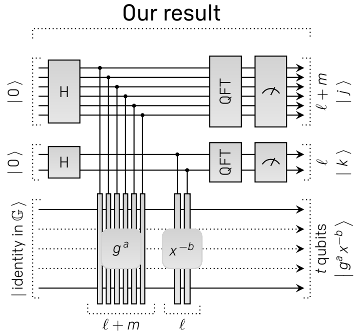
Classical post-processing

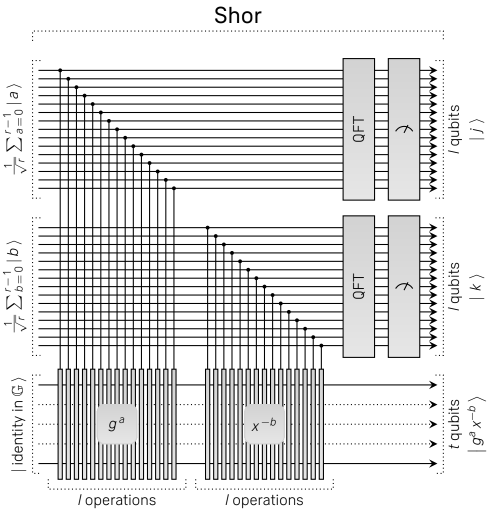
- Solve s good pairs (j, k) for d using lattice-based techniques.

- For *provable* success, execute cs times and solve all subsets of s pairs.

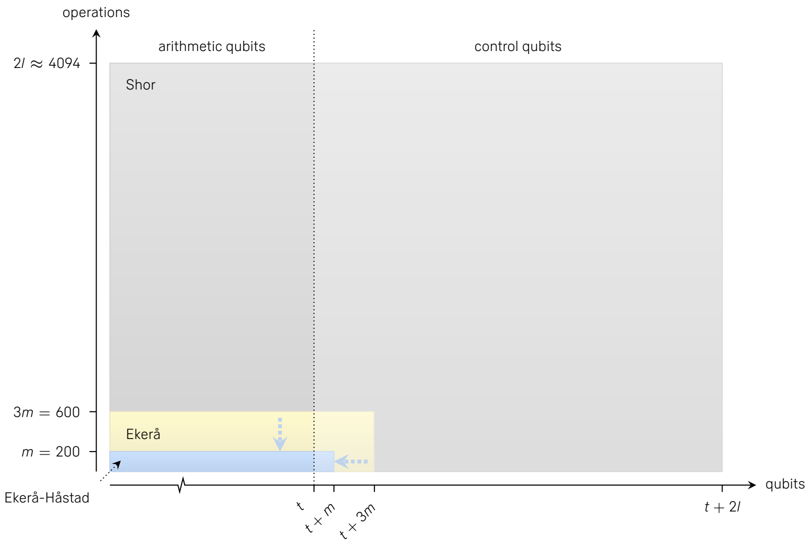
- In *practice* the condition on (j, k) may be relaxed. May trade radius for dimension.

Our advantage when solving an m bit short DLP

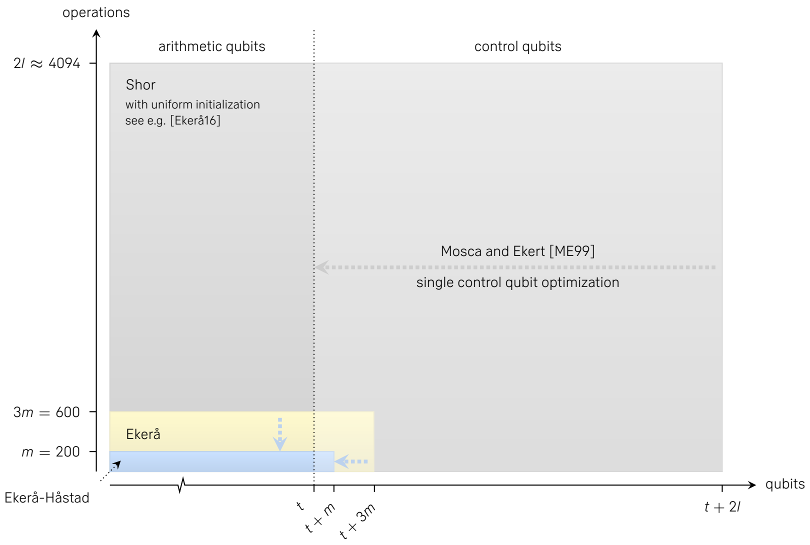




Short $m = 200$ bit DLP in safe-prime group $\mathbb{G} \subset \mathbb{F}_p^*$ for $p \approx 2^{2048}$



Short $m = 200$ bit DLP in safe-prime group $\mathbb{G} \subset \mathbb{F}_p^*$ for $p \approx 2^{2048}$



Shor's algorithm for the IFP [Shor94]

Shor's algorithm for the IFP

- Factors N by computing the order r of a random element $g \in \mathbb{Z}_N^*$.

Shor's order finding algorithm [Shor94] – *factoring* $N \in \mathbb{Z}$

1. Compute the superposition

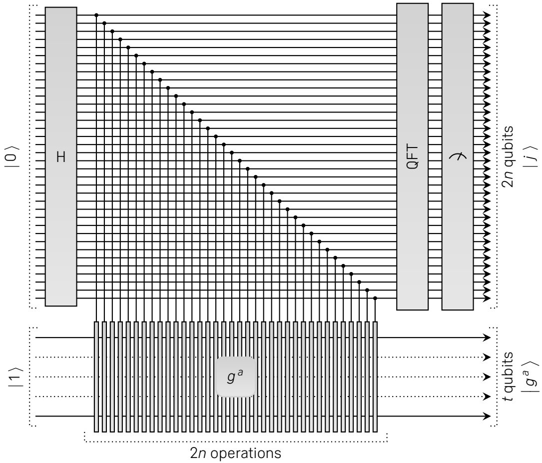
$$\frac{1}{2^n} \sum_{a=0}^{2^{2n}-1} \left| a,\, g^{a} \right\rangle$$

   where $g \in \mathbb{Z}_N^*$ and $n \sim \log_2 N$.

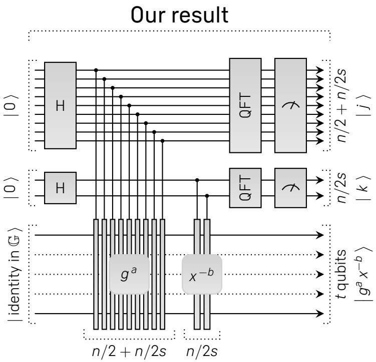
2. Compute a QFT of size 2^{2n}.
3. Observe frequency j.
4. Expect

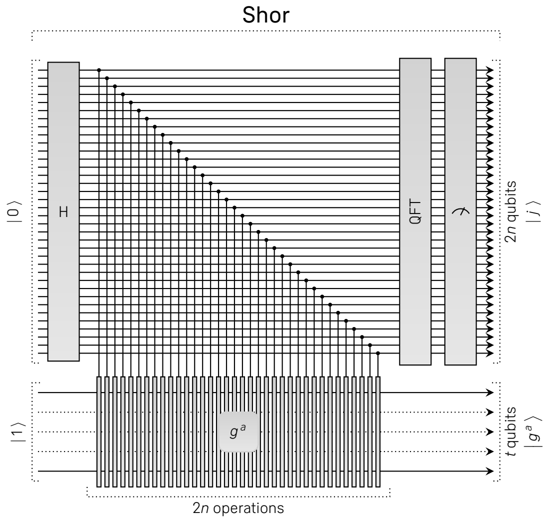
$$\frac{z}{r} \approx \frac{j}{2^{2n}} \quad \text{for some} \quad z \in \mathbb{Z}.$$

   Solve via continued fractions expansion.

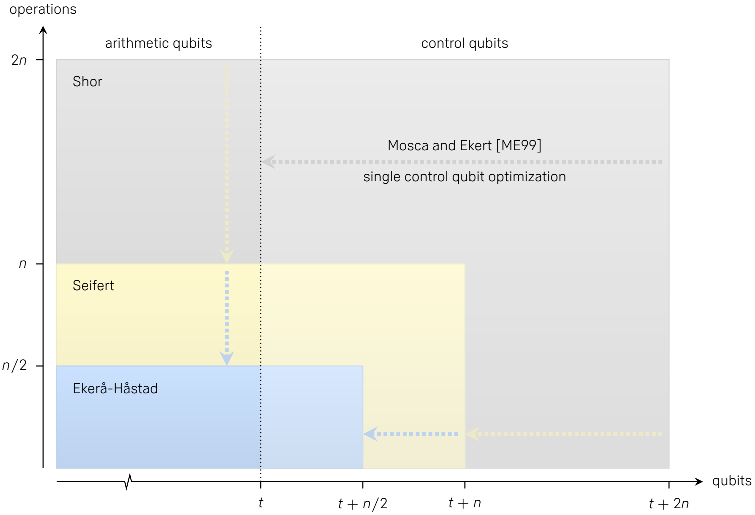


Our advantage when solving an n bit RSA IFP





Our advantage when solving an n bit RSA IFP



Summary and conclusion

Solving short m bit DLP

- Exponent reduced to $m + 2m/s$ bits for small $s \geq 1$.

- The group order may be unknown.

Factoring n bit RSA integers

- Exponent reduced from $2n$ bits to $n/2 + n/s$ bits for small $s \geq 2$.

- Reduced number of group operations, circuit depth, execution and coherence times.
- May result in a reduced number of control qubits.

Summary and conclusion

Implications for parameterization

- Safe-prime groups with short $d \sim 2^m$ yield $m + 2m/s$ bit exponents.
- Schnorr groups of order $r \sim 2^m$ yield $2m$ bit exponents.
  - Expect reduction to $m + 2m/s$ using tradeoffs.

- Not a reason to prefer safe-prime groups with short d over Schnorr groups.

Additional contributions

- We provide a full analysis of the algorithm and rigorous proofs.

KTH
VETENSKAP
OCH KONST