Hidden Shift Quantum Cryptanalysis and Implications

Xavier Bonnetain[1,2] María Naya-Plasencia[2]

[1]Sorbonne Université, France

[2]Inria, France

Outline

1. Introduction
2. New Results on Hidden Shift Algorithms
3. New Applications
4. Conclusion

Superposition attacks

Setting

- Access to quantum computing
- Access to quantum queries

Many Attacks

- Even-Mansour, [KM12]
- Many MACs, quantum slide attacks... [KLLN16]

Many Proofs

- NMAC [SY17]
- Quantum One-Way functions... [HY18]

Main Tool: Simon's Algorithm

Simon's problem

- $f : \{0,1\}^n \to \{0,1\}^n$
- $\exists s : \forall(x,y), [f(x) = f(y)] \Leftrightarrow [x \oplus y \in \{0^n, s\}]$
- Find s

Resolution

- Classical: Collision-finding — $2^{n/2}$ queries
- Quantum: Simon's algorithm — $\mathcal{O}(n)$ queries

Simon's algorithm

Quantum circuit

- *Start from* $|0\rangle|0\rangle$

Simon's algorithm

$H|x\rangle \mapsto \sum_y (-1)^{x \cdot y} |y\rangle$

Quantum circuit

- Start from $|0\rangle |0\rangle$
- *Apply H, which gives* $\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle$

Simon's algorithm

$H|x\rangle \mapsto \sum_y (-1)^{x\cdot y}|y\rangle$ $O_f|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$

Quantum circuit

- Start from $|0\rangle|0\rangle$
- Apply H, which gives $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle$
- *Apply O_f, which gives* $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle$

Simon's algorithm

$H|x\rangle \mapsto \sum_y (-1)^{x \cdot y} |y\rangle \quad O_f |x\rangle |0\rangle \mapsto |x\rangle |f(x)\rangle$

Quantum circuit

- Start from $|0\rangle |0\rangle$
- Apply H, which gives $\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle$
- Apply O_f, which gives $\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$
- *Measure the second register : we get $f(x_0)$ and project the first register to $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus s\rangle)$*

Simon's algorithm

$H|x\rangle \mapsto \sum_y (-1)^{x\cdot y}|y\rangle \quad O_f|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$

Quantum circuit

- Start from $|0\rangle|0\rangle$
- Apply H, which gives $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle$
- Apply O_f, which gives $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle$
- Measure the second register : we get $f(x_0)$ and project the first register to $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus s\rangle)$
- *Reapply H to get* $\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}(-1)^{x_0\cdot y}|y\rangle + (-1)^{(x_0\oplus s)\cdot y}|y\rangle$

Simon's algorithm

$H|x\rangle \mapsto \sum_y (-1)^{x\cdot y}|y\rangle \quad O_f|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$

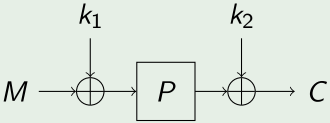
Quantum circuit

- Start from $|0\rangle|0\rangle$
- Apply H, which gives $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle$
- Apply O_f, which gives $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle$
- Measure the second register : we get $f(x_0)$ and project the first register to $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus s\rangle)$
- Reapply H to get $\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}(-1)^{x_0\cdot y}|y\rangle + (-1)^{(x_0\oplus s)\cdot y}|y\rangle$
- *The state is* $\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}(-1)^{x_0\cdot y}(1+(-1)^{s\cdot y})|y\rangle$

We measure a value y_0 such that $1+(-1)^{s\cdot y_0} \neq 0 \Rightarrow y_0 \cdot s = 0$.

Attack example

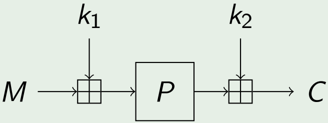
Attack on Even-Mansour [KM12]



$$f(x) = P(x) \oplus (k_2 \oplus P(x \oplus k_1))$$
$$f(x) = f(x \oplus k_1)$$

Countering the attack [AR17]

EM_+



Properties

- $f(x) = EM_+(x) + P(-x) \quad g(x) = EM_+(-x) + P(x)$
- $f(x) = g(x + k_1)$

Security

- No (known) polynomial algorithm
- Is it secure?

Hidden shift algorithms

Hidden Shift problem

- f, g permutations of $\mathbb{Z}/(2^n\mathbb{Z})$
- $f(x) = g(x+s)$
- Find s

- $2^{\mathcal{O}(\sqrt{\log(N)})}$ for $\mathbb{Z}/(N\mathbb{Z})$ [Kup05]
- $\widetilde{\mathcal{O}}(2^{\sqrt{2\log_2(3)\log_2(N)}})$ for smooth N [Kup05]
- $2^{\mathcal{O}(\sqrt{\log(N)\log(\log(N))})}$, polynomial memory [Reg04]
- $\widetilde{\mathcal{O}}(2^{\sqrt{2\log_2(N)}})$ [Kup13]

Hidden Shift in $\mathbb{Z}/(2^n\mathbb{Z})$

Oracle

$$\mathrm{O}: \begin{array}{lcl} |0\rangle\,|x\rangle\,|0\rangle & \mapsto & |0\rangle\,|x\rangle\,|f(x)\rangle \\ |1\rangle\,|x\rangle\,|0\rangle & \mapsto & |1\rangle\,|x\rangle\,|g(x)\rangle \end{array}$$

Sampling

$$\mathrm{O}\left(\sum_{i=0}^{2^n}(|0\rangle+|1\rangle)\,|i\rangle\,|0\rangle\right)=\sum_{f(x)}(|0\rangle\,|x\rangle+|1\rangle\,|x+s\rangle)\,|f(x)\rangle$$

Quantum Fourier Transform

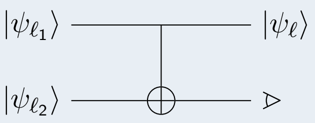
$$|\psi_\ell\rangle = |0\rangle + \exp\left(2i\pi s\frac{\ell}{2^n}\right)|1\rangle\,,\ell$$

Combining the qubits

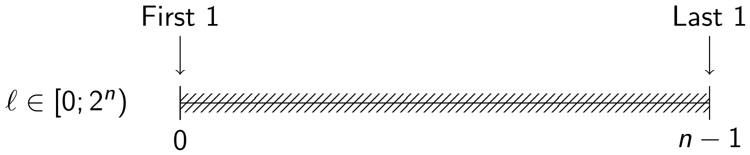
Targets

$$
\begin{aligned}
|\psi_{2^{n-1}}\rangle &= |0\rangle + (-1)^{s}\,|1\rangle \\
|\psi_{2^{n-2}}\rangle &= |0\rangle + (-1)^{\lfloor s/2 \rfloor} \exp\left(2i\pi \frac{s \mod 2}{4}\right)|1\rangle \\
&\dots
\end{aligned}
$$

Combination: CNOT



$$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2 \mod 2^n$$

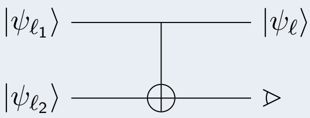


Combining the qubits

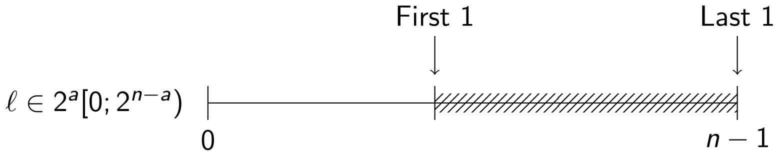
Targets

$$
\begin{aligned}
|\psi_{2^{n-1}}\rangle &= |0\rangle + (-1)^s |1\rangle \\
|\psi_{2^{n-2}}\rangle &= |0\rangle + (-1)^{\lfloor s/2 \rfloor} \exp\left(2i\pi \frac{s \mod 2}{4}\right) |1\rangle \\
&\dots
\end{aligned}
$$

Combination: CNOT



$$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2 \mod 2^n$$

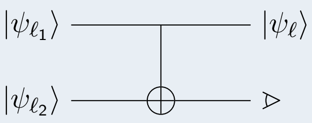


Combining the qubits

Targets

$$
\begin{aligned}
|\psi_{2^{n-1}}\rangle &= |0\rangle + (-1)^s |1\rangle \\
|\psi_{2^{n-2}}\rangle &= |0\rangle + (-1)^{\lfloor s/2 \rfloor} \exp\left(2i\pi \frac{s \mod 2}{4}\right) |1\rangle \\
&\dots
\end{aligned}
$$

Combination: CNOT



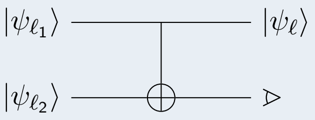
$$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2 \mod 2^n$$

Combining the qubits

Targets

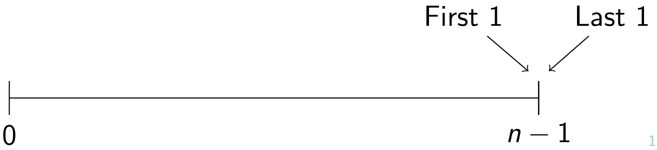
$$
\begin{aligned}
|\psi_{2^{n-1}}\rangle &= |0\rangle + (-1)^s |1\rangle \\
|\psi_{2^{n-2}}\rangle &= |0\rangle + (-1)^{\lfloor s/2 \rfloor} \exp\left(2i\pi \frac{s \mod 2}{4}\right) |1\rangle \\
&\dots
\end{aligned}
$$

Combination: CNOT



$$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2 \mod 2^n$$

$\ell \in \{0, 2^{n-1}\}$



Summary

Problem

Given quantum oracle access to f and g such that $f(x) = g(x + s)$, find s.

Asymptotic complexity [Kup05]

$\widetilde{\mathcal{O}}(2^{\sqrt{2\log_2(3)n}})$

New results

- Gain a factor n with multiple targets.
- Heuristic complexity in $2^{1.8\sqrt{n}}$
- $n > 1250$ for 2^{64} queries (Optimally: $n = 128$).

Hidden Shift in $\mathbb{Z}/(2^w\mathbb{Z})^p$

Situation

- Hidden shift $\mathbf{s} = (s_1, \ldots, s_p)$
- Elements $|\psi_{\mathbf{v}}\rangle = |0\rangle + \exp\left(2i\pi \sum_j s_j \frac{v_j}{2^n}\right)|1\rangle$

Targets

- $\left|\psi_{(2^{w-1},0\ldots,0)}\right\rangle \mapsto s_1 \mod 2$
- $\left|\psi_{(0\ldots,0,2^{w-1},2^{w-1})}\right\rangle \mapsto s_{p-1} + s_p \mod 2$
- Looking for elements in $2^{w-1}(\{0,1\}^p)$

Hidden Shift in $\mathbb{Z}/(2^w\mathbb{Z})^p$

New approach

- Looking for $(\mathbf{v_1}, \ldots, \mathbf{v_k})$ s. t. $\sum \mathbf{v_i} = \mathbf{0} \mod 2$
- Combine, obtain $\sum_i (-1)^{\delta_i} \mathbf{v_i} \in 2(\mathbb{Z}/(2^{w-1}\mathbb{Z}))^p$
- Iterate until $2^{w-1}(\{0,1\}^p)$

Complexity

- $2((p/2+1)^w)$ queries
- $w = 8 : n > 3700$ for 2^{64} queries

Combined approach

Better tradeoffs available by combining the two approaches.

Superposition attack on Poly1305

Poly1305

$\text{Poly1305}_{r,k}((m_i)_{i \leq q}) =$
$\left(\sum_{i=1}^{q}(m_{q-i+1} + 2^{128})r^i \mod 2^{130} - 5\right) + \text{E}_k(n), n$

Quantum Oracle

$|x\rangle |0\rangle \mapsto |x\rangle \left|\text{Poly1305}_{r,k}(x_1, x_2)\right\rangle, n$

Superposition attack on Poly1305

Properties

- $f(x) = \text{Poly1305}_{r,k}(0, x)$
- $g(x) = \text{Poly1305}_{r,k}(1, x)$
- $f(x + r) = g(x)$

Problems

- Group $\mathbb{Z}/((2^{130} - 5)\mathbb{Z})$
- Message constrained to $[0; 2^{128})$
- Need the same nonce for each call of f and g.

Passing through the nonce

- $f(x) = \text{Poly1305}_{r,k}(0, x)$
- $g(x) = \text{Poly1305}_{r,k}(1, x)$

Need to compute $\begin{matrix} |0, x\rangle\,|0\rangle \mapsto |0, x\rangle\,|f(x)\rangle \\ |1, x\rangle\,|0\rangle \mapsto |1, x\rangle\,|g(x)\rangle \end{matrix}$. Reduces to $|b, x\rangle\,|0\rangle \mapsto |b, x\rangle\,\big|\text{Poly1305}_{r,k}(b, x)\big\rangle$.

Constraint

Need the nonce to be independent from the input.

Group constraints

What we need

$(|0\rangle |x_0 + r\rangle + |1\rangle |x_0\rangle) |g(x_0)\rangle$

Setting

- $x < 2^{128}, r < 2^{124}$
- Problem if $x \geq 2^{128} - r$ or $x < r$

Attack

- Guess $\alpha = \lfloor \frac{r}{106} \rfloor$
- Seek a hidden shift between $f(x - 2^{106}\alpha)$ and $g(x)$.
- Need around 2^{38} quantum queries (ref: 2^{64} classical queries)

1. Introduction
2. New Results on Hidden Shift Algorithms
3. New Applications
4. **Conclusion**

Conclusion

$\oplus$ to $+$

- Generalizes many Simon-based attacks to variants
- Simon-vulnerable symmetric primitives need a huge state size.

Hidden shift

Product groups are weaker than cyclic groups

Follow-ups

- Concrete estimates for other abelian groups [ePrint 2018/537]
- Low-qubit variants