Quantum Cryptanalysis of Milenage, Telecommunications' Cryptographic Backbone

Vincent Ulitzsch[1] Jean-Pierre Seifert[1,2]

[1]Technical University Berlin, Berlin, Germany

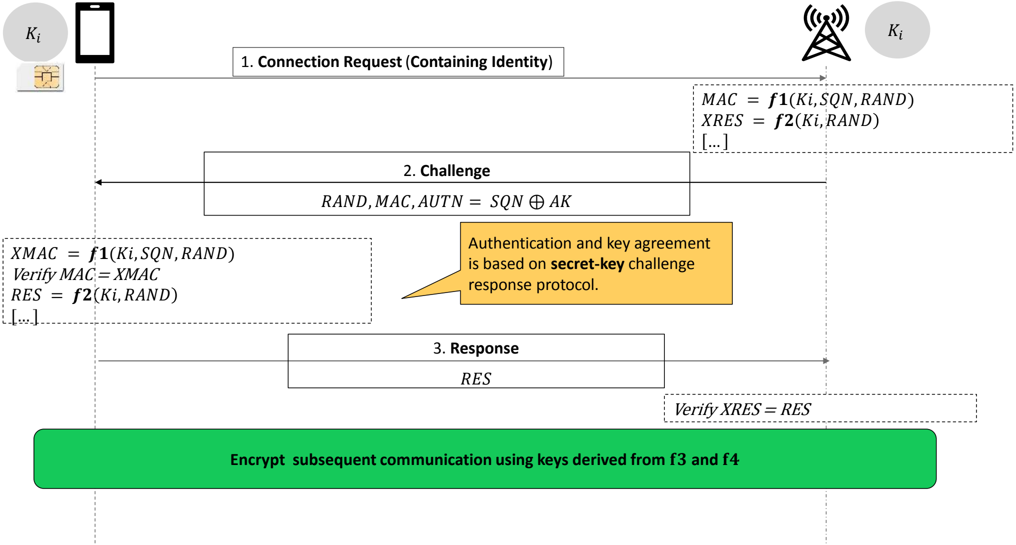
[2]Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany

August 17, 2023

Summary

- Motivation: Securing cellular networks against quantum attacks.
- Cellular networks base large chunks on secret-key cryptography, with an unexplored attack surface for quantum computers.
- Recent works present quantum cryptanalysis of symmetric cryptography that provide a speedup greater than the trivial quadratic Grover's algorithm speedup
- **Research Question** Do quantum cryptanaltic attacks extent to the secret-key cryptography used in cellular networks?

Subscriber-side security of cellular networks is rooted in the AKA protocol



- Authentication and key derivation is based on a secret-key challenge-response protocol, leveraging functions f1,..,f5.
- Most common instantiation of $f1, .., f5$: **Milenage algorithm set**: A set of secret key algorithms that base their security on AES.

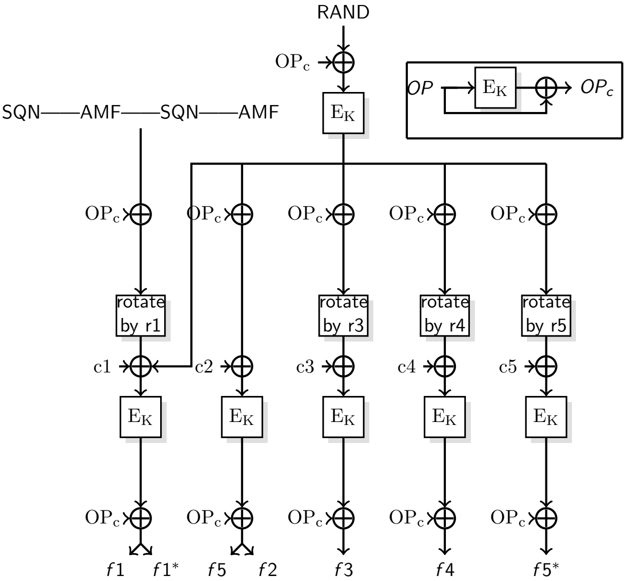
> **Research question**: Does Milenage withstand quantum cryptanalysis?

We **analyze Milenage in different dimensions**

- **Attacker Model** Quantum vs. classical oracle access, (quantum) related key access
- **Attacker Goals**: Existential forgery, (partial) key recovery

Leveraging existing quantum cryptanalysis work.

The Milenage function resembles as CBC-MAC or FX-construction



K: AES secret key shared between subscriber and operator

OP: 128-bit string, fixed per operator (secret in practice).

The $f1$ MAC resembles a CBC-MAC

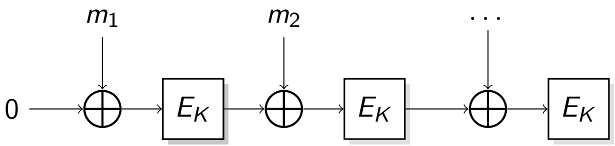


Figure: A CBC-MAC construction.

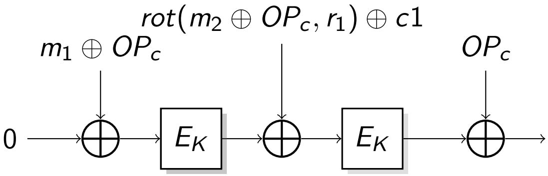


Figure: The Milenage $f1$ construction.

The $f2$ function resembles an FX-construction

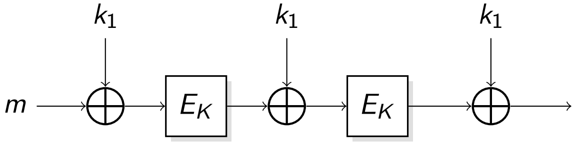


Figure: An iterated FX cipher.

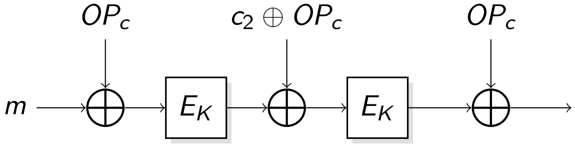


Figure: The $f2$ function, close to an iterated FX cipher.

The Milenage functions follows the structure of well-studied primitives. Do the research results extend to Milenage as well?

Quantum Cryptanalysis

- Quantum Computers provide powerful attack primitive that could lead to faster attacks against symmetric cryptography.
- Trivial attack: Grover's search, which provides quadratic speedup (albeit being hard to parallelize).
- Recent works have shown how quantum period finding can be used to go beyond that speedup.

Quantum Cryptanalysis: Speeding up Bruteforce With Grover's Algorithm

- In 1996, Grover described an algorithm that achieves a quadratic speedup when performing an unstructured, brute-force search on a quantum computer
- Can brute-force an n-bit key in $O(2^{n/2})$

> Grover's algorithm was for long only threat considered to symmetric cryptography in cellular networks. But recent results have shown that symmetric ciphers can exhibit structures that can be exploited by quantum computers in a more efficient manner.

Simon's Algorithm

Simon's algorithm: Given a periodic function, i.e. a function f where $f(x) = f(y)$ iff $x \oplus y = s$, then can **find period s in polynomial time with $O(n)$ quantum queries to f.**

- [Kaplan et al., 2016]: We can still apply Simon's algorithm even if f has some number of unwanted collisions (i.e. $f(x) = f(y)$, but $x \oplus y \neq s$)

Attacker models in quantum cryptanalysis for symmetric ciphers

Most attacks rely on Simon's algorithm – The attacks distinguish

Q1 Model "Classical" access to function f, no superposition queries – classical chosen plaintext attack
$\Rightarrow$ Simon's algorithm not directly applicable.

Q2 Model Quantum access to function – quantum chosen plaintext attack

$$\sum_{x,y} \lambda_{x,y} |x\rangle |y\rangle \rightarrow \sum_{x,y} \lambda_{x,y} |x\rangle |y \oplus f(x)\rangle$$

$\Rightarrow$ Can directly run Simon's algorithm to find period s.

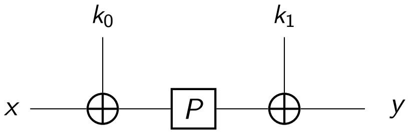
> The Q2 Model is (mostly) not practical, but encompasses all attacks possible in the Q1 Model. Thus Q2 secure implies security in all other models – which motivates this model from a security perspective.

Using Quantum Period Finding To Attack Symmetric Cryptography

A series of works established quantum attacks against symmetric cryptography using quantum period finding.

- [Kuwakado and Morii, 2012]: Quantum computers can break the classically secure Even-Mansour cipher in the $Q2$ model.
- [Kaplan et al., 2016]: CBC-MACs (and other constructions) can be broken in the $Q2$ model.
- Series of works: Speed up the attacks [Leander and May, 2017] and extend their reach to schemes where only classical access is given (Q1 model): [Bonnetain et al., 2019] and [Bonnetain et al., 2022].

Example Attack With Simon's Algorithm — The Even-Mansour Cipher



- Example quantum attack: Even-Mansour Cipher [Kuwakado and Morii, 2012]
- $E_{k_1,k_2}(x) = P(x \oplus k_0) \oplus k_1$, where P is random, but public permutation
- Can be broken with Simon's algorithm
- Attack: Construct function f such that

$$f(x) = E_{k_1,k_2}(x) \oplus P(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$$

- Clearly, this has period k_1, i.e., $f(x) = f(x \oplus k_1)$
  $\Rightarrow$ Can use Simon's algorithm to identify k_1 in polynomial time!

The offline Simon's algorithm

In the $Q1$ setting, we can also use offline Simon's algorithm [Bonnetain et al., 2019]

The offline Simon algorithm

Given

- classical oracle access to a function $g : \{0,1\}^m \to \{0,1\}^l$
- and quantum oracle access to a function $f_k\{0,1\}^n \to \{0,1\}^l$ for a guess k.
- such that $f_k \oplus g$ has a period.

Output: The offline Simon's algorithm can find k such that $f_k \oplus g$ is periodic in $O(2^m + 2^{n/2})$ time, using 2^m *classical queries*.

Offline Simon's Algorithm: Intuition

The offline Simon's algorithm [Bonnetain et al., 2019]:

1. Query g on all possible inputs to prepare a sample state $\sum_{x \in \{0,1\}^n} |x\rangle |g(x)\rangle$
2. Use Grover to guess a key k such that $f_k \oplus g$ might be periodic
3. In Grover: Use Simon's algorithm with prepared sample state to verify whether guess k led to a periodic function $f_k \oplus g$

$\Rightarrow$ With offline Simon's algorithm, can attack FX-construction $FX_{k_1,k_2,k}(x) = E_k(x \oplus k_1) \oplus k_2$ in $O(2^{\frac{m+n}{3}})$ time.

The Milenage functions follows the structure of well-studied primitives. Do the research results extend to Milenage as well?

Yes! This presentation covers two attacks on $f1$ and $f2$ respectively, details in the paper.

Attacking Milenage: Existential Forgery in the $Q2$ Model

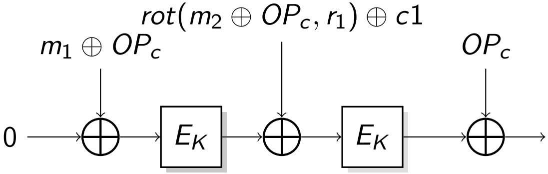


Figure: The Milenage $f1$ construction.

This is close to a CBC-MAC: Is the rotation sufficient to prevent the attack by [Kaplan et al., 2016]?

Answer: Can abuse the linearity of rotation and the fact that r_1, c_1 are public to break the scheme.

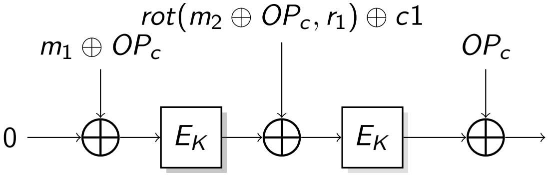


Figure: The Milenage $f1$ construction.

Attack (following [Kaplan et al., 2016]):

1. Pick two arbitrary bit-strings $\alpha_0, \alpha_1 \in \{0, 1\}^{|M|}$ with $\alpha_0 \neq \alpha_1$.
2. Define function $f' : \{0,1\} \times \{0,1\}^{|M|} \to \{0,1\}^{|M|}$ by

$$\begin{aligned} & f'(b, m_2) \\ \stackrel{\text{def}}{=} \; & f1_{K,OP_c}(\alpha_b, m_2) \\ = \; & E_K[E_K[\alpha_b \oplus OP_C] \oplus rot_{r1}(m_2) \oplus rot_{r1}(OP_c) \oplus c_1] \oplus OP_c. \end{aligned}$$

3. This function has period $(1, rot_{r1}^{-1}(\alpha_0^* \oplus \alpha_1^*))$, sufficient to perform existential forgery.

Result: In the Q_2 model, we can use Simon's algorithm for an existential forgery attack on $f1$ in quantum polynomial time.

Key Recovery Using Quantum Slide Attack

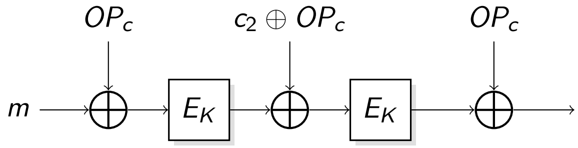


Figure: The $f2$ function, close to an iterated FX cipher.

Define $f2'(m) = f2(m \oplus c2) \oplus c2$

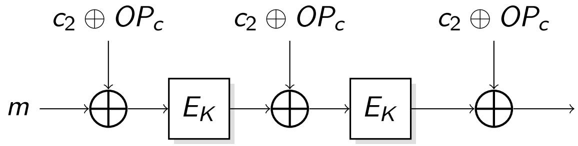


Figure: The $f2'$ function, which now resembles an iterated FX cipher.

Key Recovery Using Quantum Slide Attack

Slide Attack

Can now apply a quantum slide attack described by [Bonnetain et al., 2019] to achieve key recovery

To see why, note slide property: $f2'(E_K(x \oplus OP_c^*)) \oplus (x \oplus OP_c^*) = E_K(f2'(x)) \oplus x$

$\Rightarrow$ Can now reformulate slide property as a period function and apply (offline) Simon's algorithm!

Result: Key recovery in $\tilde{O}\left(|M| \cdot \mathtt{T}_{\mathtt{QAES}}) \cdot 2^{\frac{|K|}{2}}\right)$ time with $O(2^{|M|})$ classical queries, where $|M|$ is the challenge length and $|K|$ is the key length.

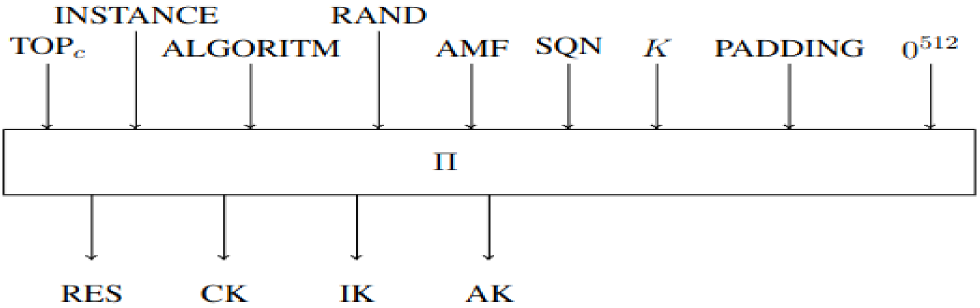
- In post-quantum configuration, with $|OP_c| = 128$, $|K| = 256$:
  Quantum Slide Attack Requires $c \cdot (2^{128} + 2^{128} \cdot \mathtt{T}_{\mathtt{QAES}})$ operations
  Grover's attack Requires $c \cdot (2^{384/2}) \cdot \mathtt{T}_{\mathtt{QAES}} = c \cdot 2^{192} \cdot \mathtt{T}_{\mathtt{QAES}}$ operations.
- Have achieved a speedup even in the $Q1$ model.

Results Summary

Attack	Model	Classical Queries	Superposition Queries	Circuit Depth Complexity
Grover's attack for key recovery, OP known	Q_1	$O(1)$	0	$O\left(2^{\lvert K\rvert/2}\cdot \mathtt{T}_{\mathtt{QAES}}\right)$
Grover's attack for key recovery, OP unknown	Q_1	$O(1)$	0	$O\left(2^{(\lvert K\rvert+\lvert OP_c\rvert)/2}\cdot \mathtt{T}_{\mathtt{QAES}}\right)$
Key Recovery $f2$, OP unknown	Q_2	0	$O(\lvert M\rvert)$	$\tilde{O}\left((\lvert M\rvert\cdot \mathtt{T}_{\mathtt{QAES}})\cdot 2^{\lvert K\rvert/2}\right)$??
Offline Key Recovery $f2$, OP unknown	Q_1	$O\left(2^{\lvert M\rvert}\right)$	0	$\tilde{O}\left(2^{\lvert M\rvert}\cdot \mathtt{T}_O + (\lvert M\rvert\cdot \mathtt{T}_{\mathtt{QAES}})\cdot 2^{\frac{\lvert K\rvert}{2}}\right)$
Existential Forgery $f1$	Q_2	$O(1)$	$O(\lvert M\rvert)$	$O(\lvert M\rvert\cdot \mathtt{T}_O)$
Related Key Attack $f1,\dots,f_5$	Q_2	0	$O(\lvert K\rvert+\lvert OP_c\rvert)$	$\tilde{O}((\lvert K\rvert+\lvert OP_c\rvert)\cdot \mathtt{T}_O)$
Offline Related Key Attack $f1,\dots,f5$	Q_1	$O\left(2^{\frac{\lvert K\rvert+\lvert OP_c\rvert}{3}}\right)$	0	$\tilde{O}(S\cdot \mathtt{T}_O + S\cdot \mathtt{T}_{\mathtt{QAES}})$ where $S=2^{\frac{\lvert K\rvert+OP_c\rvert}{3}}$

Table: Summary of the results. $\lvert K\rvert$ is the length of the message authentication key, $\lvert OP_C\rvert$ is the length of the OP_c bitstring and $\lvert M\rvert$ is the block length of the underlying block cipher. In the case of Milenage, $\lvert K\rvert=\lvert OP_C\rvert=\lvert M\rvert=128$. For all complexity estimates, the big-O notation hides only a very small multiplicative constant.

Alternative to Milenage: TUAK



The TUAK algorithm set, based on the Keccak-f permutation [Mandal et al., 2015]. There are no known quantum attacks against TUAK, even in the $Q2$ model.

Conclusion

- The Milenage algorithm exhibit structures making them susceptible to quantum period finding attacks.
- However, these *do not* imply that Milenage is broken.
- Further research is required to see if attacks or security proofs can be extended.

Thank you for your attention! Questions/Comments? vincent@sect.tu-berlin.de

References I

Bonnetain, X., Hosoyamada, A., Naya-Plasencia, M., Sasaki, Y., and Schrottenloher, A. (2019).
Quantum attacks without superposition queries: the offline Simon's algorithm.
In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 552–583. Springer.

Bonnetain, X., Schrottenloher, A., and Sibleyras, F. (2022).
Beyond quadratic speedups in quantum attacks on symmetric schemes.
In *Advances in Cryptology – EUROCRYPT 2022*, pages 315–344, Cham. Springer International Publishing.

Kaplan, M., Leurent, G., Leverrier, A., and Naya-Plasencia, M. (2016).
Breaking symmetric cryptosystems using quantum period finding.
In *Annual international cryptology conference*, pages 207–237. Springer.

References II

Kuwakado, H. and Morii, M. (2012).
Security on the quantum-type even-mansour cipher.
In *2012 International Symposium on Information Theory and its Applications*, pages 312–316. IEEE.

Leander, G. and May, A. (2017).
Grover meets Simon–quantumly attacking the FX-construction.
In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 161–178. Springer.

Mandal, K., Tan, Y., Wu, T., and Gong, G. (2015).
A comprehensive security analysis of the tuak algorithm set.