量子計算機を前提とした攻撃に対する共通鍵暗号の安全性評価に関する研究

Survey on security evaluation of symmetric encryption scheme against quantum computer attack

本原拓也・システム分科会・情報セキュリティ大学院大学

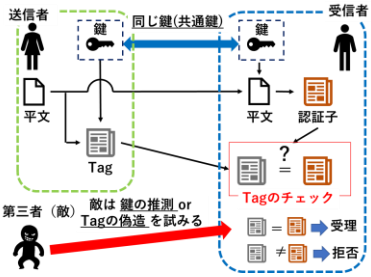
Many of research and investigations on attacks based on quantum computers were related to public key cryptography, but research and investigations on cryptographic systems other than public key cryptography also tend to increase recently. Thus ,we focus on attacks based on the quantum computer for symmetric encryption scheme, and report the security for some specific block cipher.

MAC（Message Authentication Code）とは

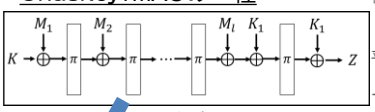
・大まかに、なりすまし・偽造を防止するための仕組み

・同じ鍵で生成したTagにより、送信者・平文の完全性を保証

・悪意のある第三者は、鍵の情報は未知であり、鍵の推測 or Tagの偽造 を試みる



Chaskey：MACの一種



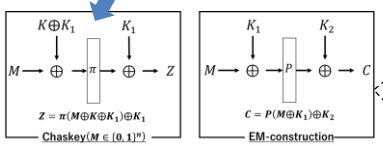
置換　$\pi: \{0,1\}^n \mapsto \{0,1\}^n$

鍵　$K \in \{0,1\}^n$　$K_1 = 2 \cdot K \in \{0,1\}^n$

平文　$M_1, M_2, \cdots, M_l \in \{0,1\}^n$　$(M_1 || M_2 || \cdots || M_l \leftarrow M)$

Tag　$Z \in \{0,1\}^n$

平文が1ブロック長だと…



平文が1ブロック長のChaskey
＝
2種類の鍵を用いたEM construction

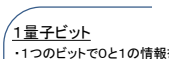
量子計算（量子ゲート型）とは

量子ビットと量子アルゴリズム（量子ゲートの組み合わせ）により、任意の問題を解く

量子ビットとは

1量子ビット

・1つのビットで0と1の情報を重ね合わせて保持
・観測という操作を行うと、初めて0か1か確定



$|\varphi\rangle = c_0|0\rangle + c_1|1\rangle$

・c_0, c_1は振幅を指し、確率の情報を保持
・$|\varphi\rangle$を観測すると
$|c_0|^2$の確率で0、$|c_1|^2$の確率で1となる

n量子ビット

$\sum_{k=0}^{2^n-1} c_k|k\rangle$　$|k\rangle = |x_0\rangle \otimes |x_1\rangle \otimes \cdots \otimes |x_{n-1}\rangle$　$k = x_0\, x_1 \cdots x_{n-1}$

$|00\cdots0\rangle \cdots |11\cdots1\rangle$に対する振幅（$c_k$）を保持
観測をすると、$|c_k|^2$の確率でkを得る

どうやって問題を解くか

・量子ゲートをうまく組み合わせc_kを制御すること
・量子ゲートの組み合わせを『量子アルゴリズム』という

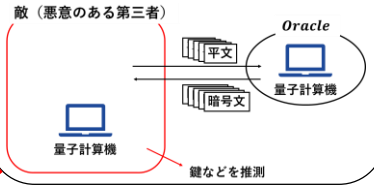
一般的な計算手順

①量子ビットをレジスタにセット
②任意の量子ゲートを繰り返しレジスタに適用（量子ビットのc_k を制御）
③レジスタを観測し、$|c_k|^2$の確率でnビットの値kを得る

攻撃モデル

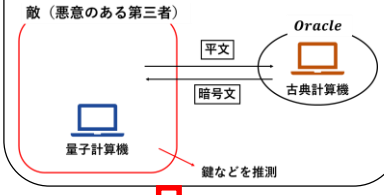
Q2モデル

・Olacleへ平文（量子ビット）を照会すると対応する暗号文（量子ビット）が返ってくる
・上記により得られた平文・暗号文の組み合わせと量子計算機を用いて、鍵などを推測する



Q1モデル

・Oracleへ平文（古典ビット）を照会すると、対応する暗号文（古典ビット）が返答される
・上記により得られた平文・暗号文の組み合わせと量子計算機を用いて、鍵などを推測する



Q2モデルのアプローチ（Chaskey）

Slide Attack ＋Simonのアルゴリズム（by Kaplan et al.）
※1ブロック分の平文を入力値とした場合のChaskeyを考える

$F: \{0,1\}^n \rightarrow \{0,1\}^n$
$F(M) = \pi(M \oplus K \oplus K_1) \oplus K_1 \oplus \pi(M)$

$F(M \oplus K \oplus K_1) = F(M)$

$F(M \oplus K \oplus K_1)$
$= \pi(M \oplus K \oplus K_1 \oplus K \oplus K_1) \oplus K_1 \oplus \pi(M \oplus K \oplus K_1)$
$= \pi(M) \oplus K_1 \oplus \pi(M \oplus K \oplus K_1)$
$= F(M)$

古典的手法（Slide Attacks）の概念に基づき、Fを定義
⇒**Simonのアルゴリズムが適用可能となる**

$s = K \oplus K_1 = 3K$（sはFの周期）

$K_1 = 2 \cdot K$

Simonのアルゴリズムを適用
周期sを求める
⇒$O(n)$で周期sが分かる

Kを取り出す

Q1モデルのアプローチ（Chaskey）

Online-Offine MitM Attack（中間一致攻撃の一種）＋Groverのアルゴリズム（by Hosoyamada et al.）
※1ブロック分の平文を入力値とした場合のChaskeyを考える

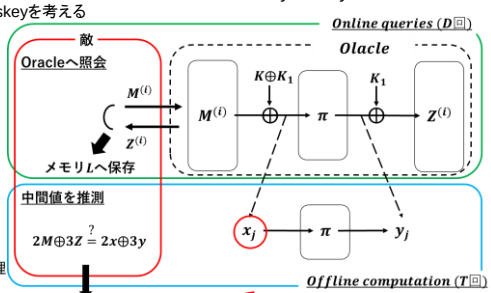
変数$x, y \in \{0,1\}^n$を定義

$x = M \oplus K \oplus K_1 \quad y = \pi(x)$

Online-Offline MitM Attackの概念より
中間値xを求める処理を次のとおり定める

【*Online Query*】：D回
・Chaskeyの暗号化オラクルへMのクエリを照会し、対応するZを得る処理
（MとZの組み合わせは、メモリLに保存）

【*Offline Computation*】：T回
・xを推測し、それに対応する$y = \pi(x)$を計算する処理



$M \oplus x \oplus y \oplus Z = K$
$K_1 = y \oplus Z = 2 \cdot K$

$M \oplus x \oplus y \oplus Z = K$
$= M \oplus (M \oplus K \oplus K_1) \oplus (\pi(x)) \oplus (\pi(x) \oplus K_1)$
$= K$

$2(M \oplus x \oplus y \oplus Z) = y \oplus Z$

$2M \oplus 3Z = 2x \oplus 3y$

【Online Query】
D個の$(M^{(i)}, Z^{(i)})$を入手
【Offline Computaion】
T個の(x_j, y_j)を入手
<左記の式が成り立つかどうかチェック>

*Online Query*の回数(D)と*Offline Computation*の回数(T)は下記のトレードオフの関係にある
$D \cdot T = N(= 2^n)$

xを推測出来れば、鍵K, K_1が判明する

安全性評価（Q2モデル）

$n, k = 128$のとき、
解読に必要な計算量は$O(128)$

⇒鍵長を2倍（128→256）としても、
多項式時間にて解読（$O(128) \rightarrow O(256)$）

安全性評価（古典計算機）

$n, k = 128$のとき、
解読に必要な計算量は計算量は$O(2^{80})$*

※中間一致攻撃の対策として、
暗号化処理を2^{48}回実行したら、鍵を更新する前提
⇒$D \cdot T = N(2^{128}), D = 2^{48}$より、$T = 2^{80}$を保証

安全性評価（Q1モデル）-Chaillouxらが提案する評価手法

・ハードウェアの実装を考慮(現実的な量子ビット数等を制限したケースを仮定
・Offline Computation（T）の処理は、「Groverのアルゴリズム」の概念を利用

$D \cdot T^6 = N^3 (D < N^{\frac{3}{7}}, using\ D^{\frac{1}{3}}\ classical\ memory)$

$n, k = 128$,鍵を2^{48}回ごとに更新するとしても、計算量$O(2^{56})$

Q2モデルにおける脅威

特定の暗号に対する影響は非常に大きいが攻撃モデルが強力であり、実際の攻撃を想定すると、非現実的な側面あり

・従来まで有効であった、鍵長を長くする等の対策が無効となる（計算量：指数時間⇒多項式時間）
・送受信者が量子計算機を利用する前提
→送受信者は、「量子計算機を利用しない」という対策が可能

公開鍵暗号に対する脅威

・公開鍵暗号(RSA,ECCなど)に関しては、数十年前に提案された『Shorのアルゴリズム』により解読可能
・攻撃者のみが量子計算機を持っていれば攻撃可能だが、取り扱う量子ビットの数が非常に多い

・約1万量子ビット程度の量子ビットが必要となる
・送受信者が古典計算機を利用する前提
→Q1と同様に、攻撃者のみが量子計算機を持てばアプローチ可能であるが、大量の量子ビットを取り扱うことが可能な量子計算機でなければならない

Q1モデルにおける脅威

Q2モデルと比較してインパクトこそ小さいが現実的なアプローチが可能

・ハードウェアへの実装・利用する量子ビットの数等を考慮したうえで、特定の暗号を現実的に解読可能とする
・送受信者が古典計算機を利用する前提
→「量子計算機を利用しない」という対策が無効
攻撃者のみが量子計算機を入手すれば攻撃可能

非現実的 ← 現実的な脅威であるかどうか → 現実的