モンゴメリ法及び並列化を適用した 耐サイドチャネル攻撃RSA復号回路の高位合成

High-Level Synthesis of Side Channel Attack Resistant RSA Decryption Circuit with Montgomery Modular Multiplication and Parallelization

大窄 直樹 Naoki Osako　　石浦 菜岐佐 Nagisa Ishiura

関西学院大学 理工学部　School of Science and Technology, Kwansei Gakuin University

1　はじめに

IoT (Internet of Things) 向け組込み機器の増加に伴い, 暗号回路のサイドチャネル攻撃への対策が重要な課題となっている. 文献 [1] では, Fournaris のアルゴリズム [2] に基づき, サイドチャネル攻撃に耐性を持つ RSA の復号回路を高位合成により設計する手法を提案しているが, 攻撃に耐性を持たせるために, 復号回路の規模, 実行時間が大幅に増加している. 本稿では, モンゴメリ法及び並列化により, サイドチャネル攻撃に耐性を持つ RSA 復号回路の高速化と回路規模の削減を試みる.

2　耐サイドチャネル攻撃 RSA 復号回路の高位合成

Fournaris のアルゴリズム (図 1) [2] は, RSA 復号処理のサイドチャネル攻撃に対する脆弱性の解決を図ったものであり, 一般的な単純電力解析攻撃や差分電力解析攻撃の他, Bellcore 攻撃, KQ 攻撃, YLMH 攻撃等の故障利用攻撃への耐性を持つ. [1] は, 多倍長整数演算ライブラリ GMP を用いて Fournaris のアルゴリズムを C 言語で記述し, これを高位合成システム ACAP [3] で合成することにより耐サイドチャネル攻撃 RSA 復号回路を設計している.

3　モンゴメリ法適用及び並列化

本稿では, モンゴメリ法の適用と並列化により [1] の RSA 復号回路を効率化する. 図 1 中の乗算剰余演算 ($x \cdot y \bmod M$) を全てモンゴメリ法での計算に変更するとともに, モンゴメリ法で使用する R, p, q 等を事前に計算して定数として与える. 図 1 の ② に 2 箇所ある FSCAME にはデータ依存がないので並列に計算する. これは, FSCAME を計算する回路モジュールを作成し, 一方の FSCAME の計算開始と同時にこれを起動することにより実現する.

4　合成結果

本稿の手法により記述した C プログラムを ACAP で高位合成し, Xilinx Vivado (2016.4) で FPGA (kintex-7 xc7k70) をターゲットとして論理合成した. 結果を表 1 に示す. RSA は攻撃に耐性のないの回路, SRR は [1] の回路, SRR+M は SRR にモンゴメリ法を適用した回路, SRR+M+P は SRR+M に並列化を適用した回路である. cycles は 128 ビット復号処理に要したサイクル数である. モンゴメリ法の適用により回路規模を約 68%に削減できた. 並列化により回路規模は SRR の 1.35 倍になったが, サイクル数は 56%に削減できた. 結果, RSA の約 5.17 倍の実行時間, 約 1.94 倍の回路規模でサイドチャネル攻撃耐性を持たせることができた.

① 耐攻撃 Montgomery 冪剰余算

Function: FSCAME
Input: $c, b, b^{-1}, d = (1, d_{t-2}, ...d_0), M$
Output: (s_0, s_1, s_2, s_4)
$R = 2^{n+2}$;　$T = R^2 \bmod M$;
$b_R = b \cdot R \bmod M$;
$b_{R-1} = b^{-1} \cdot R \bmod M$;
$s_0 = s_1 = b_R$;
$T_R = T \cdot c \cdot R^{-1} \bmod M$;
$s_2 = b_R \cdot T_R \cdot R^{-1} \bmod M$;
$s_3 = s_4 = s_5 = b_{R-1}$;
for $(i = 0$ to $t-1)$ {
　if $(d_i = 1)$ {
　　$s_0 = s_0 \cdot s_2 \cdot R^{-1} \bmod M$;　$s_4 = s_4 \cdot s_3 \cdot R^{-1} \bmod M$;
　} **else** {
　　$s_1 = s_1 \cdot s_2 \cdot R^{-1} \bmod M$;　$s_5 = s_5 \cdot s_3 \cdot R^{-1} \bmod M$;
　}
　$s_2 = s_2^2 \cdot R^{-1} \bmod M$;　　$s_3 = s_3^2 \cdot R^{-1} \bmod M$;
}
$s_0 = s_0 \cdot b^{-1} \cdot R^{-1} \bmod M$;　$s_1 = s_1 \cdot c \cdot R^{-1} \bmod M$;
$s_2 = s_2 \cdot 1 \cdot R^{-1} \bmod M$;　$s_4 = s_4 \cdot b \cdot R^{-1} \bmod M$;
if (i and d are not modified **and**
　　$s_0 \cdot s_1 \cdot R^{-1} \bmod M = s_2 \cdot 1 \cdot R^{-1} \bmod M$)
　{ **return** (s_0, s_1, s_2, s_4); } **else** { **return** error; }

② RSA 復号

Input: $c, b, b^{-1}, p, q, d_p, d_q, i_q = q^{-1} \bmod p, N$
Output: $c^d \bmod N$
$(s_0^p, s_1^p, s_2^p, s_4^p) = \text{FSCAME}(c, b, b^{-1}, d_p, p)$;
$(s_0^q, s_1^q, s_2^q, s_4^q) = \text{FSCAME}(c, b, b^{-1}, d_q, q)$;
$S_0 = s_0^q + q \cdot ((s_0^p - s_0^q) \cdot i_q \bmod p)$;
$S_1 = s_1^q + q \cdot ((s_1^p - s_1^q) \cdot i_q \bmod p)$;
$S_2 = s_2^q + q \cdot ((s_2^p - s_2^q) \cdot i_q \bmod p)$;
$S_4 = s_4^q + q \cdot ((s_4^p - s_4^q) \cdot i_q \bmod p)$;
if $(S_0 \cdot S_1 \bmod N = S_2$ **and** p, q not modified)
　{ **return** $(S_0 \cdot S_4 \bmod N)$; } **else** { **return** error; }

図 1　Fournaris のアルゴリズム [2].

表 1　合成結果.

code	#LUT	動作周波数 [MHz]	cycles
RSA	11,721	107.8	68,261
SRR [1]	16,801	77.5	627,615
SRR+M	11,464	105.5	680,284
SRR+M+P	22,727	105.6	353,489

5　むすび

本稿では, モンゴメリ法及び並列化により耐サイドチャネル攻撃 RSA 復号回路の効率化をした. 耐攻撃性の評価及び回路の更なる効率化が今後の課題である. 本研究は一部 JSPS 科研費 16K00088 の助成による.

参考文献

[1] 太田, 由良, 石浦: “電力解析攻撃/故障利用攻撃耐性 RSA 復号回路の高位合成,” 信学ソ大, A-6-6 (Sept. 2016).

[2] P. Fournaris, et al.: “Protecting CRT RSA against fault and power side channel attacks,” in *Proc. VLSI 2012*, pp. 159–164 (Aug. 2012).

[3] N. Ishiura, H. Kanbara, and H. Tomiyama: “ACAP: Binary synthesizer based on MIPS object codes,” in *Proc. ITC-CSCC 2014*, pp. 725–728 (July 2014).