REDOG 파라미터 수정

Jon-Lark Kim(PI) [1] Ji-Hoon Hong [1] Terry Shye Chien Lau [2]
Byung-Sun Won [1] Bo-seung Yang [1]

[1]Sogang University

[2]Multimedia University

October 23, 2024

Contents

1. Proposed attack

1. Proposed attack

On September 20, 2024, Alex Pellegrini presented an analysis of REDOG[1]in the Kpqc bulletin.

They proposed a message recovery attack called the "Pad Thai attack."

The Pad Thai attack is divided into two steps.

[1]Alex Pellegrini, and Marc Vorstermans, Analysis of REDOG: the Pad Thai attack. KpqC-bulletin, (September 20, 2024)

1. Proposed attack - First step.

The goal of first step is to construct a linear system of equations starting from the relation $\mathbf{c_2} = \mathbf{m}F + \mathbf{e_2}$.

They combine columns of F and the corresponding entries of $\mathbf{c} = (\mathbf{c_1}, \mathbf{c_2})$ in order to obtain a system of equations $\mathbf{c_2'} = \mathbf{m}F' + \mathbf{e_2}'$, where $\mathbf{e_2}'$ has only t_2 nonzero entries whose positions are known.

1. Proposed attack - First step.

In this part, they mentioned that the values corresponding to t_2 among the parameters of REDOG are 2 or 3. Because of this, the $n-k-t_2$ entries in $\mathbf{c}'$ are said to be error-free.

Using this fact, they can generate $F'' \in \mathbb{F}_{2^m}^{\ell \times (n-k-t_2)}$, a submatrix of F', that satisfies $\mathbf{c_2}'' = \mathbf{m}F''$ where $\mathbf{c_2}'' \in \mathbb{F}_{2^m}^{(n-k-t_2)}$.

1. Proposed attack - Second step.

In the second step, they propose a method to uniquely compute m based on the results obtained above.

They pad the system in $\mathbf{c_2}'' = \mathbf{m}F''$ with $t_2 + 1$ extra error-free equations by combining some of the equations from $\mathbf{c_1} = \mathbf{m}M + \mathbf{e_1}$ as follows:

$$(\mathbf{c_2}''|c_{1,1}|\cdots|c_{1,t_2+1}) = \mathbf{m}(F''|M_1'|\cdots|M_{t_2+1}')$$

where $c_{1,i} = \mathbf{m}M_i'$ for $i = 1, ..., t_2 + 1$.

1. Proposed attack -Overall algorithm.

The overall algorithm of Pad Thai attack is as follows:

Algorithm 2.9 PadThaiAttack

Input: A REDOG's ciphertext $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) \in \mathbb{F}_{2^m}^{2n-k}$ corresponding to a message $\mathbf{m} \in \mathbb{F}_{2^m}^{\ell}$ under the public key $\mathsf{pk} = (M \mid F) \in \mathbb{F}_{2^m}^{\ell \times (2n-k)}$.
Output: The message $\mathbf{m}$.

For each arrangement $\mathbf{a} \in A_{2t_2,n-k}$ do:

1. Let $F'', \mathbf{c}'' = \text{RearrangeSystem}(\mathbf{a})$;
2. Pick random sets $J_1, \ldots, J_{t_2+1} \subset \{1, \ldots, n\}$ with $|J_i| = t_1 + 1$;
3. Let M_{J_i} be the matrix consisting of columns of M indexed by J_i;
4. if $\mathsf{rk}(M_{J_i}) \leq t_1 + 1$ for some $i \in \{1, \ldots, t_2 + 1\}$ then go to step 2.
5. For every $(\mathbf{v}_1, \ldots, \mathbf{v}_{t_2+1}) \in \left(\mathbb{F}_2^{t_1+1}\right)^{t_2+1}$ do:
   (a) Compute $M'_i = M_{J_i}\mathbf{v}^\top$ for each $i = 1, \ldots, t_2 + 1$;
   (b) Let $\mathbf{c}_{1,J_i}$ be the vector consisting of the entries of $\mathbf{c}_1$ indexed by J_i;
   (c) Compute $c'_{1,i} = \mathbf{c}_{1,J_i}\mathbf{v}_i^\top$ for each $i = 1, \ldots, t_2 + 1$;
   (d) Let $G := (F'' \mid M'_1, \ldots, M'_{t_2+1})$ and $\mathbf{y} =$ and $\mathbf{y} := (\mathbf{c}'' \mid c'_{1,2}, \ldots, c'_{1,t_2+1}))$;
   (e) Compute $\mathbf{m}' = \mathbf{y}G^{-1}$;
   (f) Compute $\mathbf{e}'_1 = \mathbf{c}_1 - \mathbf{m}'M$ and $\mathbf{e}'_2 = \mathbf{c}_2 - \mathbf{m}'F$;
   (g) If $\mathsf{wt}_R(\mathbf{e}'_1) = t_1$ and $\mathsf{wt}_R(\mathbf{e}'_2) = t_2$ then return $\mathbf{m}' - \mathsf{hash}((\mathbf{e}'_1 \mid \mathbf{e}'_2))$.

2. Parameter modification

2. Parameter modification

The formula for the complexity of the message attack in the Pad Thai attack is as follows:

$$\mathcal{O}(2^{(t_1+1)(t_2+1)+t_2(n-k)}\ell^{\omega}m)$$

where ω is the matrix multiplication exponent.

2. Parameter modification

Due to the Pad Thai attack, the security of the parameters we previously proposed has decreased as follows:

Table: REDOG security reduced by the Pad Thai attack

Security parameter	$(n, k, \ell, q, m, r, \lambda, t_1, t_2)$	Pad Thai attack
128	(30,6,25,2,59,12,3,6,2)	87.92
192	(44,8,37,2,83,18,3,12,2)	132
256	(58,10,49,2,109,24,3,15,3)	230.53

2. Parameter modification

In the first step of the Pad Thai attack, we noted that the size of t_2 is an important factor.

We can meet the security level again with slight parameter adjustments while maintaining the REDOG scheme.

2. Parameter modification

The new parameter is as follow:

Table: Modificated parameters for REDOG

Security parameter	$(n, k, \ell, q, m, r, \lambda, t_1, t_2)$	Pad Thai attack
128	(36,6,31,2,67,15,3,6,3)	137.97
192	(47,6,43,2,89,20,3,11,3)	192.71
256	(56,10,49,2,109,24,3,11,4)	266.53

2. Parameter modification

The computational cost of the newly proposed parameters against existing attacks and Pad Thai attack is as follow:

Table: Security level and cost for each parameter of REDOG

Instance	$(n, k, \ell, q, m, r, \lambda, t_1, t_2)$	*AGHT*	*GRS*	*BBB+*	*BBC+*	*BBB* + 23	Pad Thai attack
128	(36,6,31,2,67,15,3,6,3)	258.95	289.46	144.01	209.04	170.56	137.97
192	(47,6,43,2,89,20,3,11,3)	569.90	607.90	293.04	522.41	347.07	192.71
256	(56,10,49,2,109,24,3,11,4)	729.96	779.41	322.94	624.47	382.48	266.53

2. Parameter modification

The key sizes(bytes) of the newly proposed parameters is as follow:

Table: Security level and cost for each parameter of REDOG

Security parameter	public key	secret key	ciphertext
128_{old}	4,174bytes	653bytes	376bytes
128_{new}	7,606bytes	943bytes	540bytes
192_{old}	13,658bytes	1,425bytes	820bytes
192_{new}	19,154bytes	1,671bytes	956bytes
256_{old}	31,869bytes	2,497bytes	1,436bytes
256_{new}	29,991bytes	2,352bytes	1,357bytes