A Key-Recovery Attack on a Leaky Seasign Variant

Shai Levin[1]

University of Auckland, New Zealand,
shai.levin@auckland.ac.nz

Abstract. We present a key-recovery attack on a variant of the Seasign signature scheme presented by [Kim24], which attempts to avoid rejection sampling by presampling vectors $\mathbf{f}$ such that the $\mathbf{f}-\mathbf{e}$ is contained in an acceptable bound, where $\mathbf{e}$ is the secret key. We show that this choice leads to a bias of these vectors such that, in a small number of signatures, the secret key can either be completely recovered or its keyspace substantially reduced. In particular, on average, given 20 signatures; with parameter set II of their paper; the attack reduces the private key to 128 possibilities.

Keywords: Isogeny-based cryptography · Cryptanalysis · CSIDH · Signature Schemes

1 Introduction

Seasign is an isogeny group-action based signature scheme, first proposed by De Feo and Galbraith [DG19], and later refined by [DPV19]. The scheme is derived from a sigma-protocol for a proof of knowledge of a one-way function obtained by isogeny group-actions, with the Fiat-Shamir-with-aborts transform [Lyu09] applied to obtain a signature. The security of Seasign requires rejection sampling, where the prover may restart the protocol in order to prevent leaking information about the secret. The core idea is to ensure that the responses sent by the signer, which are either ephemeral values or differences between ephemeral values and the secret key, remain within specific bounds. If a response falls outside these bounds, the signer aborts the protocol and restarts, thereby preventing any unintended leakage of information about the secret key.

However, the work by Kim [Kim24], introduces a variant of the Seasign scheme that attempts to bypass the need for rejection sampling, eliminating the potential for unnecessary computations caused by protocol aborts and restarts. The proposed variant claims to achieve this by pre-sampling commitment vectors such that responses will be distributed uniformly for either challenge bit, independent of the secret key. However, we show that this approach inadvertently introduces a bias in the distribution of the responses. The signer's attempt to avoid rejection sampling by pre-sampling commitment vectors leads to a situation where certain responses become impossible, depending on entries of the secret key.

Acknowledgements This work is supported by funding from the Ministry for Business, Innovation and Employment, New Zealand. The author would like to thank Prof. Steven Galbraith for his intuition and guidance on this work.

Notation Given an indexed set of vectors, we use $\mathbf{v}_i^{(j)}$ to refer to the i-th entry of the j-th vector. We refer to the set $\{1 \ldots n\}$ as $[n]$, and the set of integers between a and b (inclusive) as $[a, b]$.

2 The Seasign Variant in [Kim24]

Since the cryptanalysis of our work does not depend on the technical nature of isogeny-based group actions, we will not delve into the technical details of the Seasign scheme. Instead, we will briefly describe the relevant features of Seasign signature generation, and include a description of the variant proposed by Kim et al. [Kim24].

The Seasign scheme in [DG19] Seasign is based on an identification protocol where the secret key corresponds to a secret vector $\mathbf{e} \in [-B, B]^n$ which is used as input to a one-way function:

$$f(\mathbf{e}) = \mathfrak{i}_1^{\mathbf{e}_1} \ldots \mathfrak{i}_n^{\mathbf{e}_n} \star E = E'$$

where E, E' are elliptic curves, and $\mathfrak{i}_i$ are elements of the ideal class group of $\mathrm{End}(E)$, which defines a group action on the set of supersingular curves over a finite field $\mathbb{F}_p$. The public key corresponds to E', and the signature is a proof of knowledge that the signer knows the secret key $\mathbf{e}$, with the message tied into the randomness of the challenge computation.

As part of the original protocol, the signer samples, and commits to, random vectors $\mathbf{f}^{(j)} \leftarrow\!\!\$ \, [-(\delta{+}1)B, (\delta{+}1)B]^n$ for $j \in \{1, \ldots, t\}$. After receiving t single bit challenges, for each challenge c_j, the signer either sends $\mathbf{f}^{(j)}$ if $c_j = 0$ or $\mathbf{f}^{(j)} - \mathbf{e}$ if $c_j = 1$. However, for $c_j = 1$, the signer leaks some information about the vector $\mathbf{e}$, since the distribution of $\mathbf{f}^{(j)} - \mathbf{e}$ is not uniform in $[-(\delta + 1)B, (\delta + 1)B]^n$. To avoid this, rejection sampling is used. After computing the challenge, if a response vector, which is either $\mathbf{f}^{(j)}$ or $\mathbf{f}^{(j)} - \mathbf{e}$, is not in the bound $[-\delta B, \delta B]^n$, the signer aborts the protocol and restarts. This is repeated until the signer sends a valid response.

Modifications to Signature Generation in [DPV19] The approach is refined in the follow up work [DPV19] where aborts are avoided in the case that $c_j = 0$, since this only reveals the ephemeral values $\mathbf{f}^{(j)}$, and leak nothing about the secret. Furthermore, given t iterations of the sigma protocol, their protocol tolerates up to u aborts (for $u < t$) before the protocol must be re-executed, which substantially improves signature generation efficiency.

Modifications to Signature Generation in [Kim24] The approach of [Kim24] differs from these two prior works by attempting to avoid rejection sampling completely, by presampling commitment vectors $\mathbf{f}^{(1)}, \ldots, \mathbf{f}^{(t)}$ such that $\mathbf{f}^{(j)} - \mathbf{e} \in [-\delta B, \delta B]^n$. Since the signer would not need to abort and restart the protocol, this would prevent unnecessary isogeny computations, speeding up signing time. However, the key difference is that the signer cannot know what the challenge bits will be in advance, and cannot prevent bias in the distributions of the responses.

Algorithm 1 Signature Generation in [Kim24]

Input: message m, $pk = (E, E_A)$, secret key $\mathbf{e} \in [-B, B]^n$
Output: $\sigma = (\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(t)}, c_1, \ldots, c_t)$ ▷ $\mathbf{z}^{(j)} \in [-(\delta+1)B, (\delta+1)B]^n, c_j \in \{0,1\}$

$\text{cnt} \leftarrow 1$
while $\text{cnt} \leq t$ **do**
  $\mathbf{f}^{(\text{cnt})} \leftarrow\$ [-(\delta+1)B, (\delta+1)B]^n$
  $b \leftarrow \mathbf{f}^{(\text{cnt})} - \mathbf{e}$
  if $b \in [-\delta B, \delta B]^n$ **then** ▷ Resample if out of acceptable bound
    $\mathbf{z}^{(\text{cnt})} \leftarrow \mathbf{f}^{(\text{cnt})}$
    $E_{\text{cnt}} \leftarrow \mathfrak{i}_1^{\mathbf{f}_1^{(\text{cnt})}} \cdots \mathfrak{i}_n^{\mathbf{f}_n^{(\text{cnt})}} \star E$
    $\text{cnt} \leftarrow \text{cnt} + 1$
  end if
end while
$c_1, \ldots, c_t \leftarrow H(j(E_1), \ldots, j(E_t), m)$ ▷ Compute the challenge bits
for j from 1 to t **do**
  if $c_j = 0$ **then**
    $\mathbf{z}^{(j)} \leftarrow \mathbf{z}^{(j)}$ ▷ The leaky case, if $c_j = 0$
  else
    $\mathbf{z}^{(j)} \leftarrow \mathbf{z}^{(j)} - \mathbf{e}$
  end if
end for

3 The Attack

We now state an attack on signatures generated by Algorithm 1. Suppose that we are given samples

$$\mathbf{f} \leftarrow\$ [-(\delta+1)B, (\delta+1)B^n], \text{ such that } \mathbf{f} - \mathbf{e} \in [-\delta B, \delta B]^n$$

for a fixed, uniform secret $e \in [-B, B]^n$. The first observation is that, if

$$\mathbf{f} \in [-(\delta-1)B, (\delta-1)B]^n,$$

then the vector $\mathbf{f}$ leaks no information about the secret. The entries of a vector which leak information about the secret key are the entries i such that

$$(\delta-1)B < |\mathbf{f}_i| \leq (\delta+1)B,$$

i.e. the set of entries which are distance B from the threshold of the distribution. Now, suppose you are given m samples $\mathbf{f}^{(1)}, \ldots, \mathbf{f}^{(m)}$. We define

$$a_i = \min_{j \in [m]} \left(\mathbf{f}_i^{(j)} + \delta B, B \right) \qquad\qquad b_i = \max_{j \in [n]} \left(\mathbf{f}_i^{(j)} - \delta B, -B \right) \tag{1}$$

Theorem 1. *Given m vectors $\{\mathbf{f}^{(j)}\}_{j\in[m]}$ such that, for all $j \in [m]$ and some fixed $\mathbf{e} \in [-B, B]^n$, it holds that $\mathbf{f}^{(j)} \in [-(\delta+1)B, (\delta+1)B]^n$ and $\mathbf{f}^{(j)} - \mathbf{e} \in [-\delta B, \delta B]^n$. Then for $i \in [n]$ and a_i's and b_i's computed as per Equation (1), we have that:*

1. *If $a_i = b_i$, then $\mathbf{e}_i = a_i = b_i$.*
2. *If $a_i \neq b_i$ then $\mathbf{e}_i \in [b_i, a_i]$.*

Proof. Suppose that $\mathbf{e}_i \notin [b_i, a_i]$. Since $\mathbf{e}_i \in [-B, B]$, we consider either the case that:

$\mathbf{e}_i < b_i$: in which case $b_i \neq -B$ (since $\mathbf{e}_i \geq -B$), and there exists some maximal $\mathbf{f}_i^{(j)}$ such that $\mathbf{f}_i^{(j)} = b_i + \delta B$. Then $\mathbf{f}_i^{(j)} - \mathbf{e}_i = b_i + \delta B - \mathbf{e}_i > \delta B$, which contradicts the assumption that $\mathbf{f}^{(j)} - \mathbf{e} \in [-\delta B, \delta B]$.

$\mathbf{e}_i > a_i$: in which case $a_i \neq B$ (since $\mathbf{e}_i \leq B$), and there exists some minimal $\mathbf{f}_i^{(j)}$ such that $\mathbf{f}_i^{(j)} = a_i - \delta B$. Then $\mathbf{f}_i^{(j)} - \mathbf{e}_i = a_i - \delta B - \mathbf{e}_i < -\delta B$, which contradicts the assumption that $\mathbf{f}^{(j)} - \mathbf{e} \in [-\delta B, \delta B]$. □

Hence the attack is as follows. On input s signatures $\sigma_1, \ldots, \sigma_s$:

1. From each signature, collect the vectors $z^{(j)}$ for which $c_j = 0$. Set m to be the total number of such vectors.
2. For each $i \in [n]$, compute a_i and b_i as per Equation (1). Output the set of guesses for $\mathbf{e}$ as $\bigoplus_{i=1}^{n} [b_i, a_i]$.

4 Implementation and Benchmarks

We implement the key-recovery attack using a sage script available at `https://github.com/levanin/leakysea-public`. On each iteration of the experiment, a random key is sampled and a fixed number of biased samples are generated. The protocol of [Kim24] only leaks a biased vector when a challenge bit is 0, which occurs with probability $\frac{1}{2}$. So we will assume that given s signatures with challenge length t, we may obtain $\left\lfloor \frac{st}{2} \right\rfloor$ biased vectors.

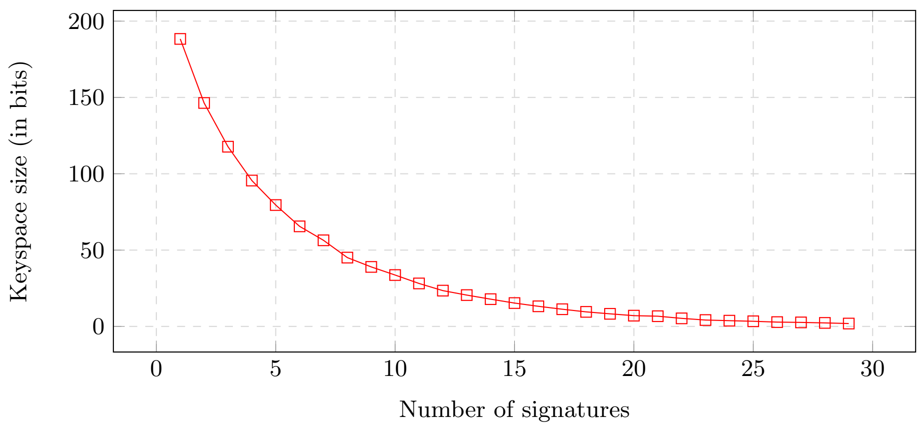

Fig. 1: Results of our attack on [Kim24, Parameter Set II]. Results are the mean over 100 random instances. The keyspace refers to the bit-length of the size of the set of possible secret keys (i.e., if the keyspace is n bits, then the number of possible secret keys is 2^n).

The attack is efficient, and all of our benchmarking was comfortably performed on a laptop over a lunch break. We provide the results of our attack given a varying number of signatures on the parameter sets provided by [Kim24] in Figures 1 and 2, obtained from the prior works [DPV19, DG19]. Once the keyspace has been reduced to a size 2^b, a meet-in-the-middle search strategy can be used to recover the secret key in time $O(2^{b/2})$, using techniques described in [DG19].

We note that the parameter set I requires a larger number of signatures to effectively perform the attack. This parameter set is designed to handle the high failure probability of the original Seasign protocol, so ephemeral vectors must be sampled from a much larger space. Hence, there is a lower chance of receiving "good" vectors which leak information about the secret key. We remark that it would have be unreasonable to use these parameters over parameter set II in the first place, since they do not yield any performance benefits over existing work. In particular, the performance of the prior work [DPV19] using parameter set

II is roughly 10× faster (2, 195 s) than the performance of [Kim24] running on parameter set I (27, 685.92 s), with claimed equivalent security levels.

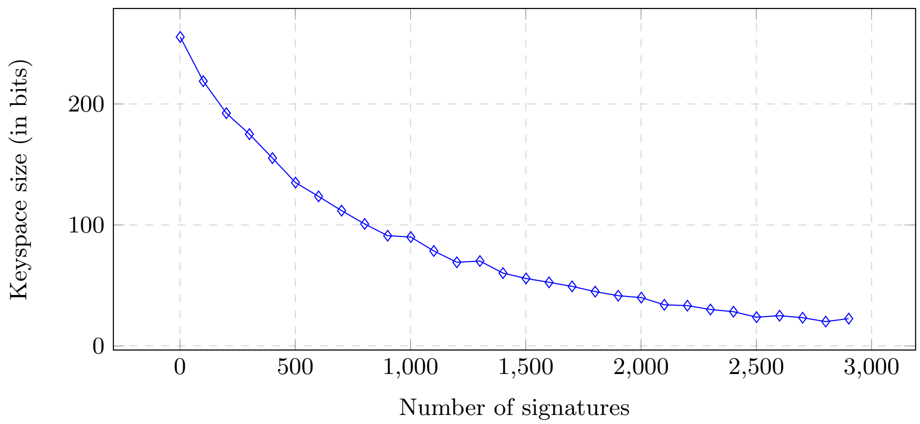

Fig. 2: Results of our attack on [Kim24, Parameter Set I]. Results are the mean over 20 random instances.

References

DG19. Luca De Feo and Steven D. Galbraith. SeaSign: Compact isogeny signatures from class group actions. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part III*, volume 11478 of *LNCS*, pages 759–789. Springer, Cham, May 2019.

DPV19. Thomas Decru, Lorenz Panny, and Frederik Vercauteren. Faster SeaSign signatures through improved rejection sampling. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019*, pages 271–285. Springer, Cham, 2019.

Kim24. Suhri Kim. Optimized seasign for enhanced efficiency. *IEEE Access*, 12:18851–18857, 2024.

Lyu09. Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 598–616. Springer, Berlin, Heidelberg, December 2009.