Speedier snail signatures

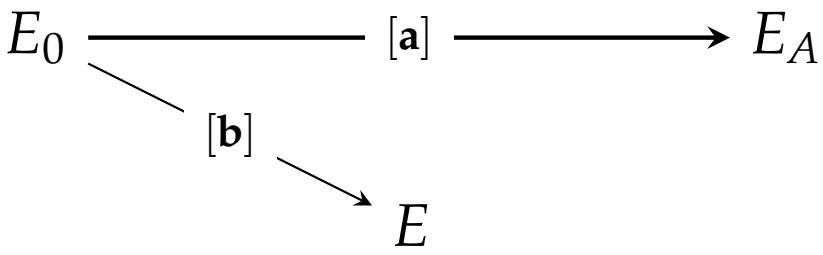
Thomas Decru Lorenz Panny Frederik Vercauteren

SeaSign [De Feo–Galbraith]

ID scheme from group actions [Couveignes, Stolbunov]:

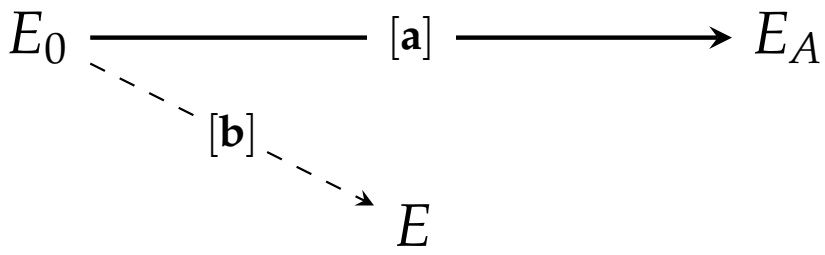
SeaSign [De Feo–Galbraith]

ID scheme from group actions [Couveignes, Stolbunov]:



SeaSign [De Feo–Galbraith]

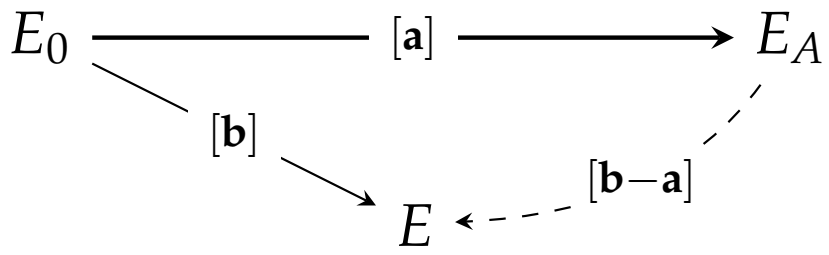
ID scheme from group actions [Couveignes, Stolbunov]:



$c = 0$: Reveal [**b**].

SeaSign [De Feo–Galbraith]

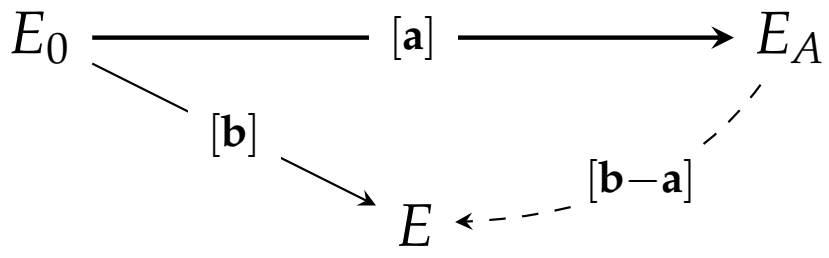
ID scheme from group actions [Couveignes, Stolbunov]:



$c = 0$: Reveal $[\mathbf{b}]$.
$c = 1$: Reveal $[\mathbf{b} - \mathbf{a}]$.

SeaSign [De Feo–Galbraith]

ID scheme from group actions [Couveignes, Stolbunov]:

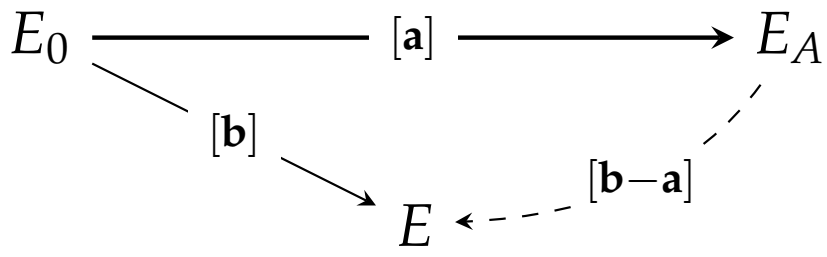


$c = 0$: Reveal $[\mathbf{b}]$.
$c = 1$: Reveal $[\mathbf{b} - \mathbf{a}]$.

- Problem: How to represent $\mathbf{b} - \mathbf{a}$ without leaking? (Distribution of $\mathbf{b} - \mathbf{a}$ depends on $\mathbf{a}$!)

SeaSign [De Feo–Galbraith]

ID scheme from group actions [Couveignes, Stolbunov]:

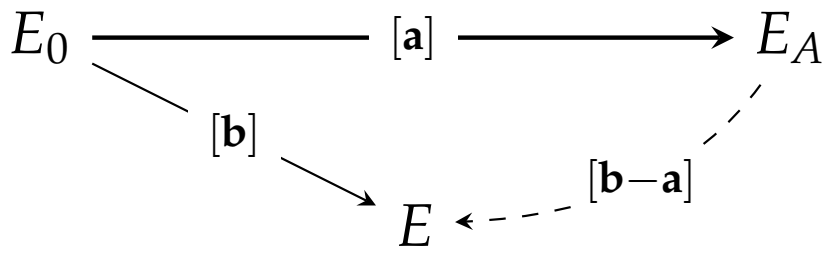


$c = 0$: Reveal $[\mathbf{b}]$.
$c = 1$: Reveal $[\mathbf{b} - \mathbf{a}]$.

- Problem: How to represent $\mathbf{b} - \mathbf{a}$ without leaking? (Distribution of $\mathbf{b} - \mathbf{a}$ depends on $\mathbf{a}$!)
- Recall: CSIDH uses vectors $\mathbf{e} \in \mathbb{Z}^n$ to represent $\left[\prod_{i=1}^{n} \ell_i^{e_i}\right]$.

SeaSign [De Feo–Galbraith]

ID scheme from group actions [Couveignes, Stolbunov]:



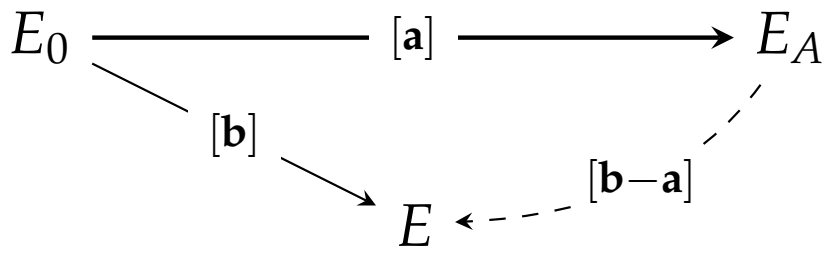
$c = 0$: Reveal $[\mathbf{b}]$.
$c = 1$: Reveal $[\mathbf{b} - \mathbf{a}]$.

- Problem: How to represent $\mathbf{b} - \mathbf{a}$ without leaking? (Distribution of $\mathbf{b} - \mathbf{a}$ depends on $\mathbf{a}$!)
- Recall: CSIDH uses vectors $\mathbf{e} \in \mathbb{Z}^n$ to represent $\left[\prod_{i=1}^{n} \ell_i^{e_i}\right]$.

$\rightsquigarrow$ The *SeaSign* scheme takes $\mathbf{b}$ in a big box $\subseteq \mathbb{Z}^n$ and rejects a query $c = 1$ when $\mathbf{b} - \mathbf{a}$ is close to the border.

SeaSign [De Feo–Galbraith]

ID scheme from group actions [Couveignes, Stolbunov]:



$c = 0$: Reveal $[\mathbf{b}]$.
$c = 1$: Reveal $[\mathbf{b} - \mathbf{a}]$.

- Problem: How to represent $\mathbf{b} - \mathbf{a}$ without leaking?
  (Distribution of $\mathbf{b} - \mathbf{a}$ depends on $\mathbf{a}$!)
- Recall: CSIDH uses vectors $\mathbf{e} \in \mathbb{Z}^n$ to represent $\left[\prod_{i=1}^{n} \ell_i^{e_i}\right]$.

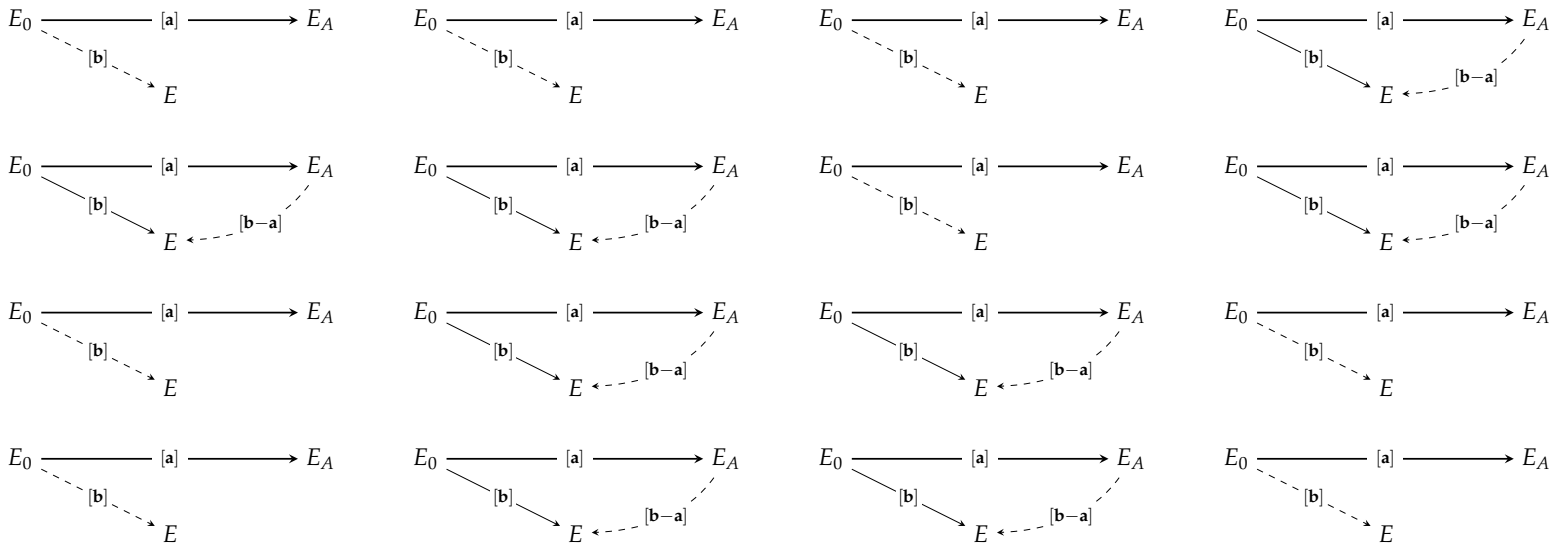
$\rightsquigarrow$ The *SeaSign* scheme takes $\mathbf{b}$ in a big box $\subseteq \mathbb{Z}^n$
and rejects a query $c = 1$ when $\mathbf{b} - \mathbf{a}$ is close to the border.

$\rightsquigarrow$ Distribution of revealed vectors $\mathbf{b} - \mathbf{a}$ is independent of $\mathbf{a}$.

- ...but tiny rejection probabilities require huge boxes.

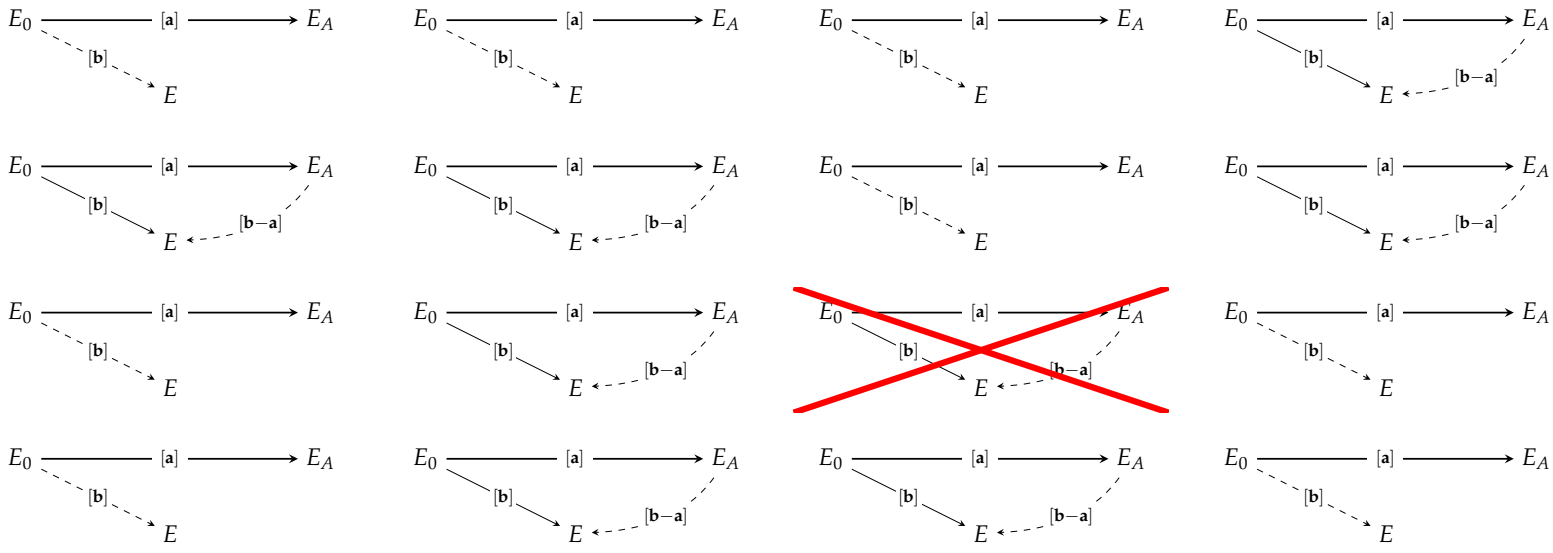
SeaSign [De Feo–Galbraith]

- $\lambda \geq 0$ independent executions give λ bits of security.



SeaSign [De Feo–Galbraith]

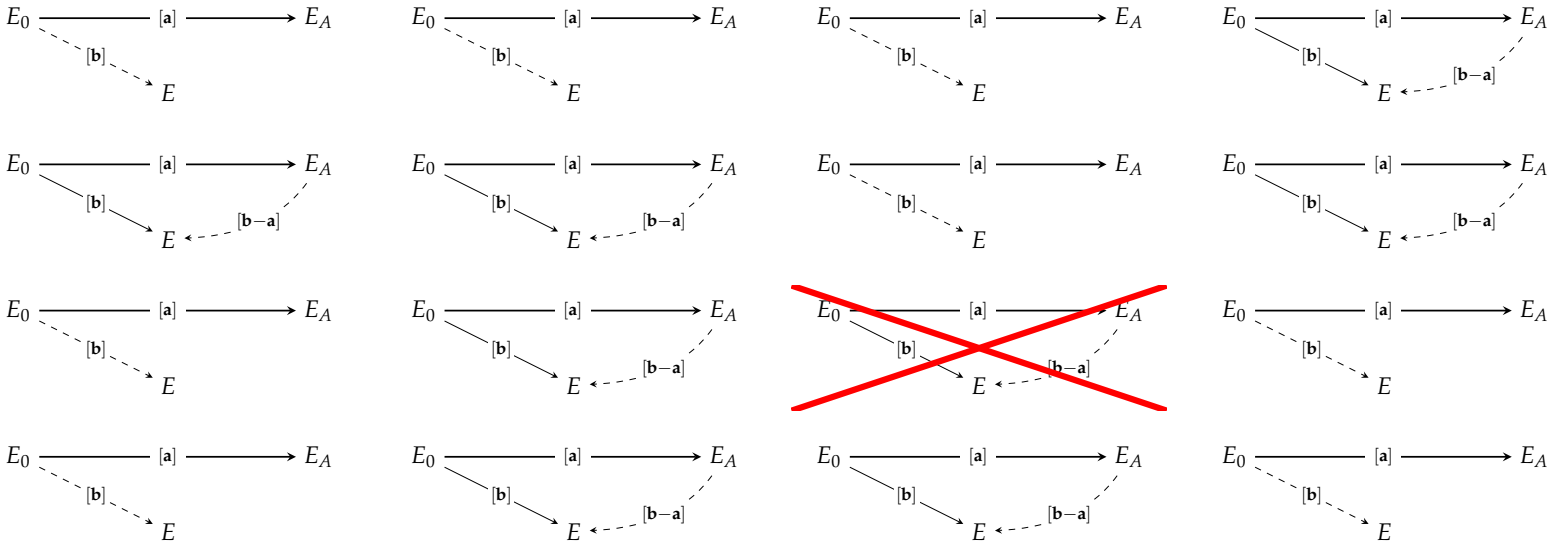
- $\lambda \geq 0$ independent executions give λ bits of security.



- SeaSign: A single rejection ✗ spoils the whole thing.

Faster SeaSign [us]

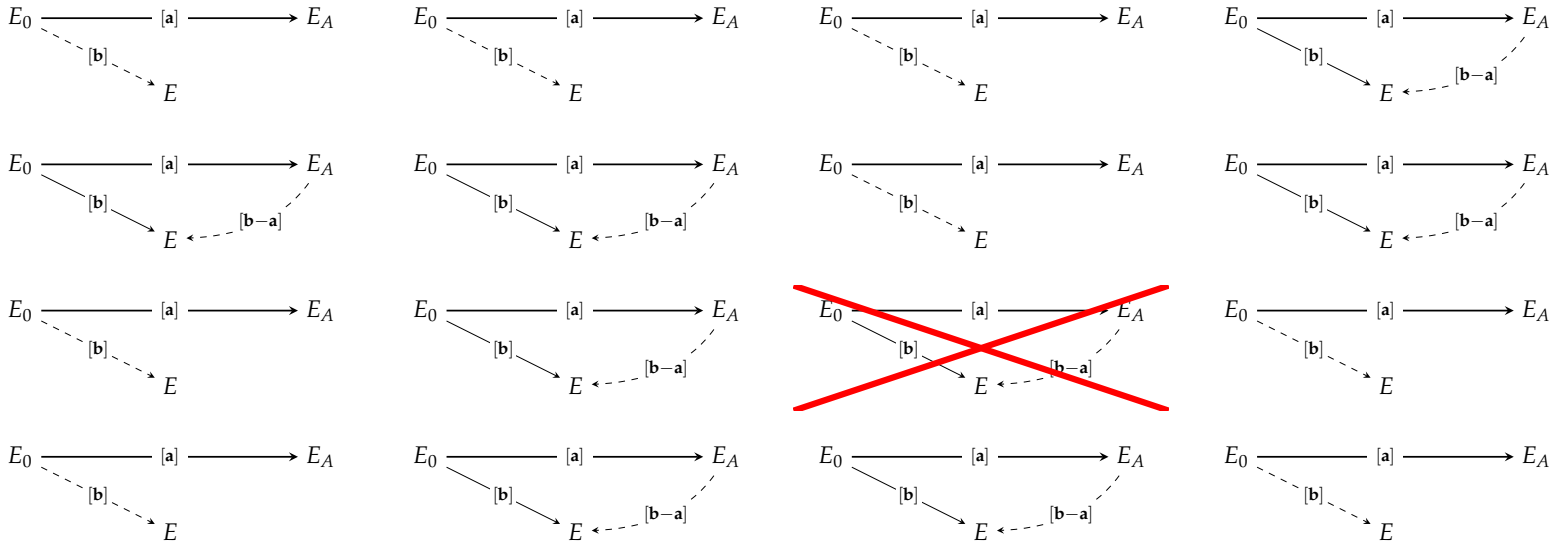
- $\lambda \geq 0$ independent executions give λ bits of security.



- SeaSign: A single rejection ✗ spoils the whole thing.
- Our idea: Why not allow 'a few' rejections?

Faster SeaSign [us]

- $\lambda \geq 0$ independent executions give λ bits of security.



- SeaSign: A single rejection ✗ spoils the whole thing.
- Our idea: Why not allow 'a few' rejections?

$\rightsquigarrow$ need $> \lambda$ correct answers, but can use smaller boxes.
$\rightsquigarrow$ better performance overall!

Thomas Decru, Lorenz Panny, Frederik Vercauteren:

Faster SeaSign signatures through improved rejection sampling

https://ia.cr/2018/1109

Thomas Decru, Lorenz Panny, Frederik Vercauteren:

Faster* SeaSign signatures through improved rejection sampling

https://ia.cr/2018/1109

* (still slow)

Thomas Decru, Lorenz Panny, Frederik Vercauteren:

Faster* SeaSign signatures through improved rejection sampling

https://ia.cr/2018/1109

* (still slow)
(but faster)

Thomas Decru, Lorenz Panny, Frederik Vercauteren:

Faster* SeaSign signatures through improved rejection sampling

https://ia.cr/2018/1109

* (still slow)
(but faster)
(between 4× and 65× faster)

Thomas Decru, Lorenz Panny, Frederik Vercauteren:

Faster* SeaSign signatures through improved rejection sampling

https://ia.cr/2018/1109

* (still slow)
(but faster)
(between 4× and 65× faster)
(which is still slow)