Accelerating Bliss: the geometry of random binary polynomials

Léo Ducas

University of California, San Diego

CHES'14, Rump Session

BLISS: a Lattice Based Signature Scheme

Comparison in Software (Our prototype[1] vs. oppenssl).

Scheme	Sign (ms)	Sign/s	Ver (ms)	Ver/s
BLISS-I	0.124	8k	0.030	33k
RSA 4096	8.660	0.1k	0.138	7.5k
ECDSA 256	0.106	9.5k	0.384	2.5k

BLISS already competes with standards, on Software [DDLL13] and on Hardware [PDG14].

Can we make it **even faster** ?

[1] Not fully optimized (e.g. no use of SSE vectorialization)

BLISS [DDL13] rejection rate

To avoid leakage BLISS repeats its main loop M times,

$$M = \exp\left(B^2/2\sigma^2\right)$$

where $\|\mathbf{S}\cdot\mathbf{c}\|_2 \leqslant B$ for any secret $\mathbf{S} \in \mathcal{S}$ and any challenge $\mathbf{c} \in \mathcal{C}$.

BLISS	**0**	**I**	**II**	**III**	**IV**
Security	Toy	128 bits	128 bits	160 bits	192 bits
Optimized for	Fun	Speed	Size	Sec.	Sec.
n	256	512	512	512	512
Repetition rate	**7.4**	**1.6**	**7.4**	**2.8**	**5.2**

Improving the bound B (with a proof !) immediately speeds up the scheme.

Geometry of polynomials

For binary random $\mathbf{S} \in \mathbb{Z}^{n \times n}$ and $\mathbf{c} \in \mathbb{Z}^n$ we have:

$$\|\mathbf{S} \cdot \mathbf{c}\|_2 \leqslant B = n \cdot (1 + o(1))$$

but for random binary **polynomials** $s, c \in \mathbb{Z}[X]/(X^n + 1)$ it is worse:

$$\|s \cdot c\|_2 \leqslant B = n \cdot \omega\left(\sqrt{\log n}\right) \quad (\approx 6n)$$

Rejecting some secrets $s \in \mathcal{S}$, [DDLL13] reached:

$$\|s \cdot c\|_2 \leqslant 1.6n.$$

Experiments suggest that this bounds it **isn't tight**.

Rejecting Challenge

To improve on that bound, we can also reject some challenges, but this rejection needs to be **independent of the secret key**.

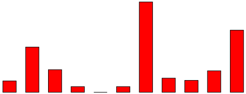
We carefully craft subsets $\mathcal{S}' \subset \mathcal{S}$, $\mathcal{C}' \subset \mathcal{C}$ and prove:

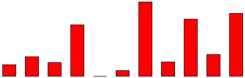
$$\|s \cdot c\|_2 \leqslant 1.2n \quad \text{for all } s \in \mathcal{S}', c \in C'.$$

General Idea

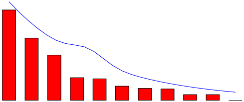
$\hat{x}$ denote $FFT(x)$. We set $\mathcal{S}' = \mathcal{C}' = \{x / \mathrm{Sort}(|\hat{x}|) \leqslant \text{Profile}\}$.

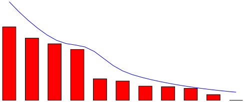
FFT(secret) : $|\hat{s}|$ $\times$ FFT(challenge) : $|\hat{c}|$ $\leqslant$



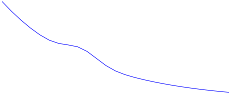


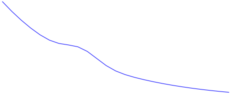
Sort($|\hat{s}|$) $\times$ Sort($|\hat{c}|$) $\leqslant$





Profile $\times$ Profile $\leqslant 1.2n$





Result

Improved speed up to a factor **2.5**.

BLISS-F	**0**	**I**	**II**	**III**	**IV**
Security	Toy	128 bits	128 bits	160 bits	192 bits
Optimized for	Fun	Speed	Size	Sec.	Sec.
speed-up	**2.2**	**1.2**	**2.4**	**1.6**	**2.5**

To appear soon on eprint. With **Open Source** implementation.

Thanks !