G+G: A Fiat-Shamir Lattice Signature Based on Convolved Gaussians

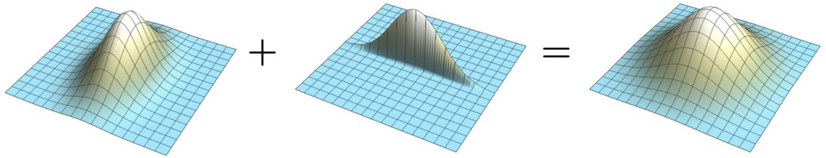
Julien Devevey
ANSSI
France

Alain Passelègue
CryptoLab Inc.
France

Damien Stehlé
CryptoLab Inc.
France

Our contributions

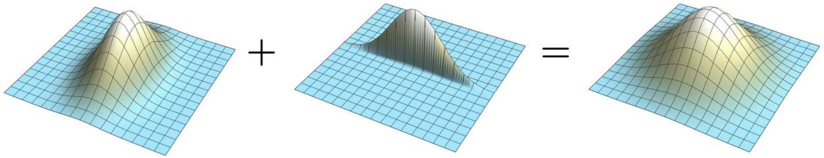
- **New technique** for building **Fiat-Shamir lattice-based signatures,** a.k.a. Lyubashevsky's signatures
- **No** rejection sampling, **no** noise flooding
- We rely on **Gaussian convolutions**



Paradigm	Scheme	Signature size	Aborts
Rejection sampling	Dilithium, HAETAE, ...	**Small** (~2kB)	YES
Noise flooding	Raccoon	Large (~15kB)	**NO**
This work	**G+G**	**Small (~2kB)**	**NO**

Our contributions

- **New technique** for building **Fiat-Shamir lattice-based signatures,** a.k.a. Lyubashevsky's signatures
- **No** rejection sampling, **no** noise flooding
- We rely on **Gaussian convolutions**



Paradigm	Scheme	Signature size	Aborts
Rejection sampling	Dilithium, HAETAE, ...	**Small** (~2kB)	YES
Noise flooding	Raccoon	Large (~15kB)	**NO**
This work	**G+G**	**Small (~2kB)**	**NO**

- proofs of signatures are subtle [DFPS23, BBD+23]
- complicates design of advanced applications (e.g. threshold signatures)

Lyubashevsky's signatures in a nutshell

- A lattice adaptation of Schnorr's identification protocol/signature
- Introduced by Lyubashevsky in 2009 [Lyu'09, Lyu'11]

Discrete logarithm problem: $\longrightarrow$ **SIS/LWE problem**

Given g, g^x find x $\longrightarrow$ Given $\mathbf{A}, \mathbf{AS}$ for $\mathbf{S}$ **small**, find $\mathbf{S}$

Lattice-based identification protocol

Prover

$\mathbf{A} \leftarrow \mathbb{Z}_q^{m\times k}$

$\mathbf{S} \leftarrow \mathbb{Z}^{k\times \ell}$ **small**

Verifier

$\mathbf{A}$, $\mathbf{T} := \mathbf{A}\mathbf{S}$

Lattice-based identification protocol

Prover

$\mathbf{A} \leftarrow \mathbb{Z}_q^{m\times k}$

$\mathbf{S} \leftarrow \mathbb{Z}^{k\times \ell}$ small

Verifier

$\mathbf{A}\ ,\mathbf{T} := \mathbf{AS}$

$\mathbf{y} \leftarrow \mathbb{Z}^k$ small

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q \longrightarrow$

Lattice-based identification protocol

Prover

$\mathbf{A} \leftarrow \mathbb{Z}_q^{m\times k}$

$\mathbf{S} \leftarrow \mathbb{Z}^{k\times \ell}$ small

Verifier

$\mathbf{A}$, $\mathbf{T} := \mathbf{AS}$

$\mathbf{y} \leftarrow \mathbb{Z}^k$ small

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

Lattice-based identification protocol

Prover

$\mathbf{A} \leftarrow \mathbb{Z}_q^{m \times k}$

$\mathbf{S} \leftarrow \mathbb{Z}^{k \times \ell}$ small

Verifier

$\mathbf{A}\ ,\mathbf{T} := \mathbf{AS}$

$\mathbf{y} \leftarrow \mathbb{Z}^k$ small

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} \bmod q \longrightarrow$

Lattice-based identification protocol

Prover

$\mathbf{A} \leftarrow \mathbb{Z}_q^{m \times k}$

$\mathbf{S} \leftarrow \mathbb{Z}^{k \times \ell}$ small

Verifier

$\mathbf{A}$, $\mathbf{T} := \mathbf{AS}$

$\mathbf{y} \leftarrow \mathbb{Z}^k$ small

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} \bmod q \longrightarrow$

Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + \mathbf{Tc} \bmod q$

Lattice-based identification protocol

Prover

$\mathbf{A} \leftarrow \mathbb{Z}_q^{m \times k}$

$\mathbf{S} \leftarrow \mathbb{Z}^{k \times \ell}$ small

Verifier

$\mathbf{A}$, $\mathbf{T} := \mathbf{AS}$

$\boxed{\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} \bmod q \longrightarrow$

Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + \mathbf{Tc} \bmod q$

Resulting signature

Prover

$$\mathbf{A} \leftarrow \mathbb{Z}_q^{m \times k}$$
$$\mathbf{S} \leftarrow \mathbb{Z}^{k \times \ell} \quad \text{small}$$

Verifier

$$\mathbf{A}\ ,\ \mathbf{T} := \mathbf{A}\mathbf{S}$$

$$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$$
$$\mathbf{w} \leftarrow \mathbf{A}\mathbf{y} \bmod q$$

$$\mathbf{c} \leftarrow H(\mathbf{A}, \mathbf{T}, \mathbf{w}, \mu)$$

$$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c} \bmod q \xrightarrow{\mathsf{Sign}(\mathbf{A}, \mathbf{S}, \mu) = (\mathbf{w}, \mathbf{c}, \mathbf{z})}$$

Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{A}\mathbf{z} = \mathbf{w} + \mathbf{T}\mathbf{c} \bmod q$

Resulting signature

Prover

$\mathbf{A} \leftarrow \mathbb{Z}_q^{m \times k}$

$\mathbf{S} \leftarrow \mathbb{Z}^{k \times \ell}$ small

Verifier

$\mathbf{A}\ , \mathbf{T} := \mathbf{AS}$

$$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k, \sigma}$$

$$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q$$

$$\mathbf{c} \leftarrow H(\mathbf{A}, \mathbf{T}, \mathbf{w}, \mu)$$

$$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} \bmod q \xrightarrow{\mathsf{Sign}(\mathbf{A}, \mathbf{S}, \mu) = (\cancel{\mathbf{w}}, \mathbf{c}, \mathbf{z})}$$

Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{c} \leftarrow H(\mathbf{A}, \mathbf{T}, \underbrace{\mathbf{Az} - \mathbf{Tc}}_{= \mathbf{w} \bmod q}, \mu)$

Properties of this protocol

Prover

$\mathbf{A}, \mathbf{S}$

Verifier

$\mathbf{A}, \mathbf{T} := \mathbf{AS}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} \bmod q \longrightarrow$

Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + \mathbf{Tc} \bmod q$

Properties of this protocol

Prover

$\mathbf{A}, \mathbf{S}$

Verifier

$\mathbf{A}, \mathbf{T} := \mathbf{A}\mathbf{S}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{y} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c} \bmod q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{A}\mathbf{z} = \mathbf{w} + \mathbf{T}\mathbf{c} \bmod q$

Completeness:

$$\mathbf{A}\mathbf{z} = \mathbf{A}(\mathbf{y} + \mathbf{S}\mathbf{c}) = \mathbf{w} + \mathbf{T}\mathbf{c} \bmod q$$

$\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c}$ is small

Properties of this protocol

Prover	*Verifier*
$\mathbf{A}$, $\mathbf{S}$	$\mathbf{A}$, $\mathbf{T} := \mathbf{AS}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} \bmod q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + \mathbf{Tc} \bmod q$

Completeness:

$$\mathbf{Az} = \mathbf{A}(\mathbf{y} + \mathbf{Sc}) = \mathbf{w} + \mathbf{Tc} \bmod q$$

$\mathbf{z} = \mathbf{y} + \mathbf{Sc}$ is small

Soundness:

From the hardness of SIS (or LWE)

Properties of this protocol

Prover

$\mathbf{A}$, $\mathbf{S}$

Verifier

$\mathbf{A}$, $\mathbf{T} := \mathbf{AS}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} \bmod q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + \mathbf{Tc} \bmod q$

Completeness:

$$\mathbf{Az} = \mathbf{A}(\mathbf{y} + \mathbf{Sc}) = \mathbf{w} + \mathbf{Tc} \bmod q$$

$\mathbf{z} = \mathbf{y} + \mathbf{Sc}$ is small

Soundness:

From the hardness of SIS (or LWE)

Zero-knowledge:

This is the focus of this talk!

Honest-Verifier Zero-knowledge

Prover

$\mathbf{A}, \mathbf{S}$

Verifier

$\mathbf{A}, \mathbf{T} := \mathbf{AS}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} \bmod q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + \mathbf{Tc} \bmod q$

"A real transcript contains no more information that what is already contained in the challenge and verification key"

Honest-Verifier Zero-knowledge

Prover

$\mathbf{A}, \mathbf{S}$

Verifier

$\mathbf{A}, \mathbf{T} := \mathbf{AS}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} \bmod q \longrightarrow$

Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + \mathbf{Tc} \bmod q$

"A real transcript contains no more information that what is already contained in the challenge and verification key"

There exists a PPT simulator Sim satisfying the following:

Input: $\mathbf{A}, \mathbf{T}, \mathbf{c}$

Output: $\mathbf{w}, \mathbf{c}, \mathbf{z}$

Honest-Verifier Zero-knowledge

Prover | ***Verifier***

$\mathbf{A}$, $\mathbf{S}$ | $\mathbf{A}$, $\mathbf{T} := \mathbf{AS}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} \bmod q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + \mathbf{Tc} \bmod q$

"A real transcript contains no more information that what is already contained in the challenge and verification key"

There exists a PPT simulator Sim satisfying the following:

Input: $\mathbf{A}, \mathbf{T}, \mathbf{c}$

Output: $\mathbf{w}, \mathbf{c}, \mathbf{z}$

<u>Indistinguishability of transcripts:</u>

$$\Delta(((\mathbf{w},\mathbf{c},\mathbf{z}) \leftarrow (\mathsf{P}(\mathbf{A},\mathbf{S}) \leftrightarrow \mathsf{V}(\mathbf{A},\mathbf{T}))), \mathsf{Sim}(\mathbf{A},\mathbf{T},\mathbf{c})) \leq \epsilon$$

or

$$\mathsf{RD}(((\mathbf{w},\mathbf{c},\mathbf{z}) \leftarrow (\mathsf{P}(\mathbf{A},\mathbf{S}) \leftrightarrow \mathsf{V}(\mathbf{A},\mathbf{T}))) \mid \mathsf{Sim}(\mathbf{A},\mathbf{T},\mathbf{c})) \leq 1+\epsilon$$

Simulation

Prover

$\mathbf{A}$, $\mathbf{S}$

Verifier

$\mathbf{A}$, $\mathbf{T} := \mathbf{A}\mathbf{S}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{y} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c} \bmod q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{A}\mathbf{z} = \mathbf{w} + \mathbf{T}\mathbf{c} \bmod q$

<u>Simulation strategy:</u>

Sim$(\mathbf{A}, \mathbf{T}, \mathbf{c})$:

Return $(\mathbf{w}, \mathbf{c}, \mathbf{z})$

Simulation

Prover

$\mathbf{A}\,,\mathbf{S}$

Verifier

$\mathbf{A}\,,\mathbf{T} := \mathbf{A}\mathbf{S}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{y} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c} \bmod q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{A}\mathbf{z} = \mathbf{w} + \mathbf{T}\mathbf{c} \bmod q$

Simulation strategy:

Sim$(\mathbf{A},\mathbf{T},\mathbf{c})$:

$\mathbf{z} \leftarrow \mathcal{D}_{\mathbf{z}}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c} \bmod q$ $\longleftarrow$ Enforced by completeness

Return $(\mathbf{w},\mathbf{c},\mathbf{z})$

Simulation

Prover

$\mathbf{A}$, $\mathbf{S}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{y} \bmod q \longrightarrow$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c} \bmod q \longrightarrow$

Verifier

$\mathbf{A}$, $\mathbf{T} := \mathbf{A}\mathbf{S}$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{A}\mathbf{z} = \mathbf{w} + \mathbf{T}\mathbf{c} \bmod q$

Simulation strategy:

Sim$(\mathbf{A}, \mathbf{T}, \mathbf{c})$:

$\mathbf{z} \leftarrow \mathcal{D}_{\mathbf{z}}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c} \bmod q$

Return $(\mathbf{w}, \mathbf{c}, \mathbf{z})$

What is the correct distribution?

Must be sampled from without $\mathbf{S}$

Enforced by completeness

Simulation

Prover

$\mathbf{A}\,,\mathbf{S}$

Verifier

$\mathbf{A}\,,\mathbf{T} := \mathbf{AS}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} \bmod q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + \mathbf{Tc} \bmod q$

Simulation strategy:

$\mathsf{Sim}(\mathbf{A}, \mathbf{T}, \mathbf{c})$:

$\mathbf{z} \leftarrow \mathcal{D}_{\mathbf{z}}$

$\mathbf{w} \leftarrow \mathbf{Az} - \mathbf{Tc} \bmod q$

Return $(\mathbf{w}, \mathbf{c}, \mathbf{z})$

What is the correct distribution?

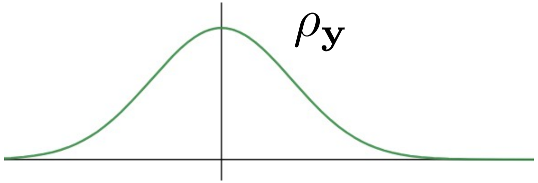
Must be sampled from without $\mathbf{S}$

Enforced by completeness

In the real protocol:

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc}$

Simulation



$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{y} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c} \bmod q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{A}\mathbf{z} = \mathbf{w} + \mathbf{T}\mathbf{c} \bmod q$

Simulation strategy:

Sim$(\mathbf{A}, \mathbf{T}, \mathbf{c})$:

$\mathbf{z} \leftarrow \mathcal{D}_{\mathbf{z}}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c} \bmod q$

Return $(\mathbf{w}, \mathbf{c}, \mathbf{z})$

What is the correct distribution?

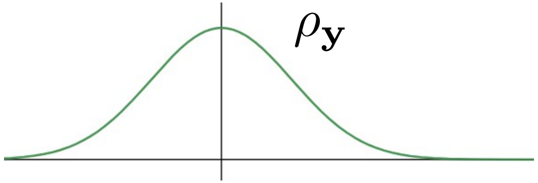
Must be sampled from without $\mathbf{S}$

Enforced by completeness

In the real protocol:

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c}$

Simulation



$\rho_{\mathbf{y}}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

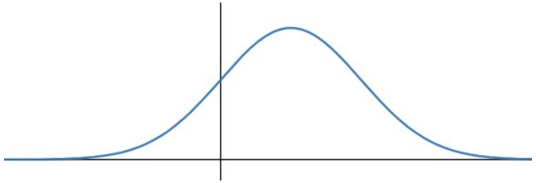
$\mathbf{w} \leftarrow \mathbf{A}\mathbf{y} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^{\ell})$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c} \bmod q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{A}\mathbf{z} = \mathbf{w} + \mathbf{T}\mathbf{c} \bmod q$



$\rho_{\mathbf{y}+\mathbf{S}\mathbf{c}}$

Simulation strategy:

$\mathsf{Sim}(\mathbf{A}, \mathbf{T}, \mathbf{c})$:

$\mathbf{z} \leftarrow \mathcal{D}_{\mathbf{z}}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c} \bmod q$

Return $(\mathbf{w}, \mathbf{c}, \mathbf{z})$

What is the correct distribution?

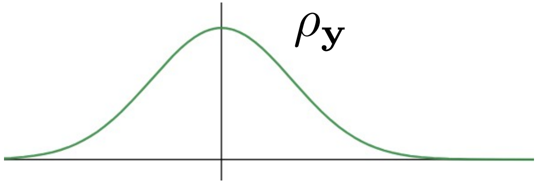
Must be sampled from without $\mathbf{S}$

Enforced by completeness

In the real protocol:

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c}$

Simulation



$\rho_{\mathbf{y}}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

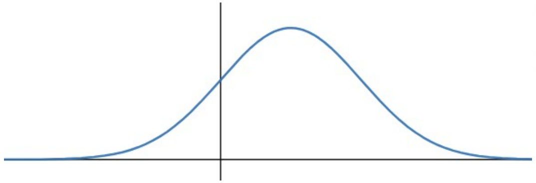
$\mathbf{w} \leftarrow \mathbf{A}\mathbf{y} \bmod q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c} \bmod q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{A}\mathbf{z} = \mathbf{w} + \mathbf{T}\mathbf{c} \bmod q$



$\rho_{\mathbf{y}+\mathbf{S}\mathbf{c}}$

Simulation strategy:

Sim$(\mathbf{A}, \mathbf{T}, \mathbf{c})$:

$\mathbf{z} \leftarrow \mathcal{D}_{\mathbf{z}}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c} \bmod q$

Return $(\mathbf{w}, \mathbf{c}, \mathbf{z})$

What is the correct distribution?

Must be sampled from without $\mathbf{S}$

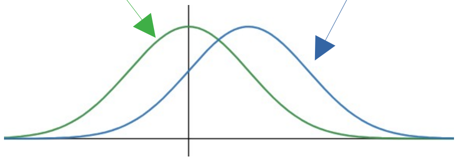
Enforced by completeness

In the real protocol:

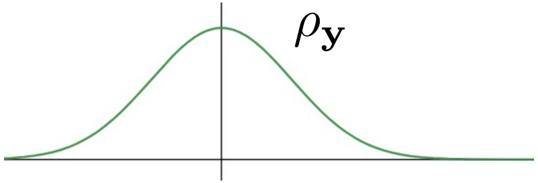
$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c}$

$\mathcal{D}_{\mathbf{z}} = \mathcal{D}_{\mathbb{Z}^k,\sigma,\mathbf{S}\mathbf{c}}$

$\rho_{\mathbf{y}}$ $\rho_{\mathbf{y}+\mathbf{S}\mathbf{c}}$



Simulation



$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

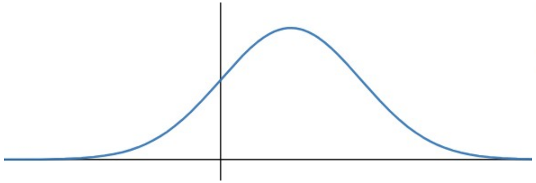
$\mathbf{w} \leftarrow \mathbf{A}\mathbf{y} \bmod q \longrightarrow$

$\longleftarrow \quad \mathbf{c} \leftarrow U(\{0,1\}^{\ell})$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c} \bmod q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{A}\mathbf{z} = \mathbf{w} + \mathbf{T}\mathbf{c} \bmod q$



<u>Simulation strategy:</u>

$\mathsf{Sim}(\mathbf{A}, \mathbf{T}, \mathbf{c})$:

$\mathbf{z} \leftarrow \mathcal{D}_{\mathbf{z}}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c} \bmod q$

Return $(\mathbf{w}, \mathbf{c}, \mathbf{z})$

What is the correct distribution?

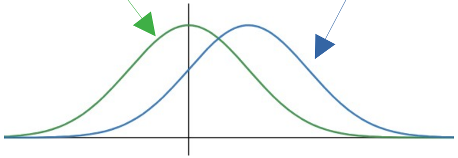
Must be sampled from without $\mathbf{S}$

Enforced by completeness

<u>In the real protocol:</u>

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c}$

$\mathcal{D}_{\mathbf{z}} = \mathcal{D}_{\mathbb{Z}^k,\sigma,\mathbf{S}\mathbf{c}}$

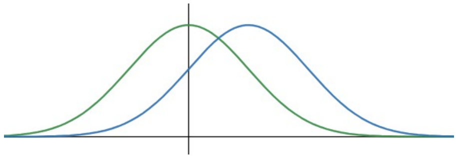


<u>The protocol is actually not always secure</u>

Two known approaches

Problem: we want to be able to sample from the distribution of $\mathbf{z}$ without knowing $\mathbf{S}$

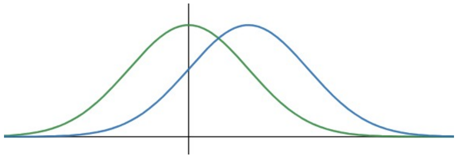
$$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c}$$



Two known approaches

Problem: we want to be able to sample from the distribution of $\mathbf{z}$ without knowing $\mathbf{S}$

$$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c}$$



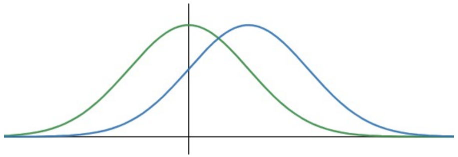
Solution 1: choose the distribution of $\mathbf{y}$ such that it remains close when shifted by $\mathbf{S}\mathbf{c}$

Make $\mathbf{y}$ much larger than $\mathbf{S}\mathbf{c}$ but still small compared to q. *This requires large parameters...*

Two known approaches

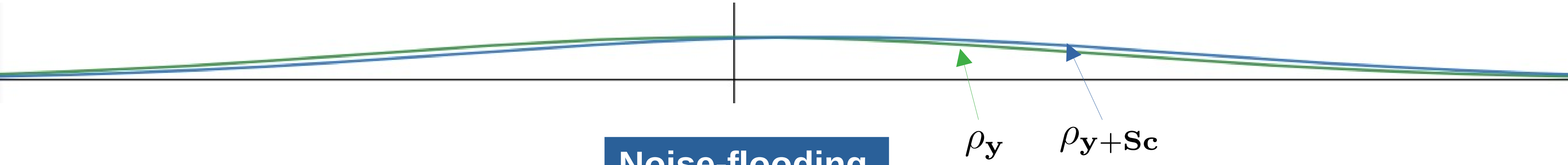
Problem: we want to be able to sample from the distribution of $\mathbf{z}$ without knowing $\mathbf{S}$

$$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc}$$



Solution 1: choose the distribution of $\mathbf{y}$ such that it remains close when shifted by $\mathbf{Sc}$

Make $\mathbf{y}$ much larger than $\mathbf{Sc}$ but still small compared to q. *This requires large parameters...*

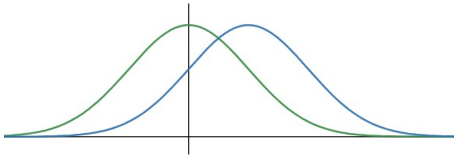


Noise-flooding

Two known approaches

Problem: we want to be able to sample from the distribution of $\mathbf{z}$ without knowing $\mathbf{S}$

$$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c}$$

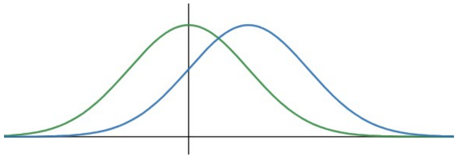


Solution 2: make the distribution of $\mathbf{z}$ independent of $\mathbf{S}\mathbf{c}$ by rejecting to a target distribution

Two known approaches

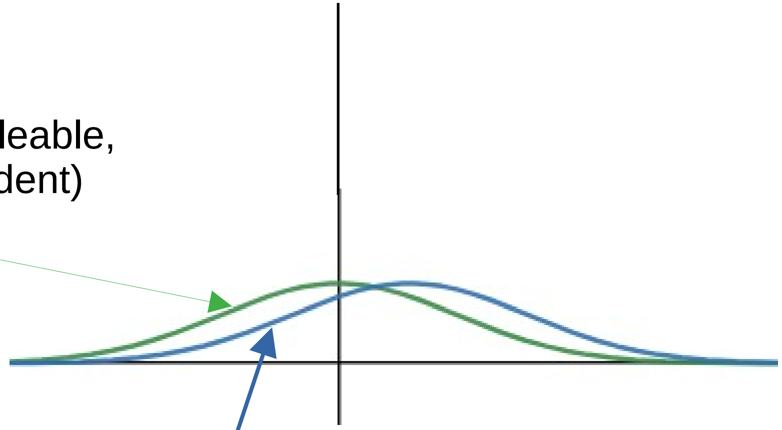
Problem: we want to be able to sample from the distribution of $\mathbf{z}$ without knowing $\mathbf{S}$

$$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c}$$



Solution 2: make the distribution of $\mathbf{z}$ independent of $\mathbf{S}\mathbf{c}$ by rejecting to a target distribution

(publicly sampleable,
key-independent)
$\rho_{\mathbf{y}}$

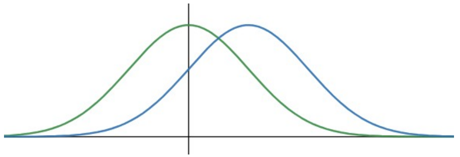


$\rho_{\mathbf{y}+\mathbf{S}\mathbf{c}}$

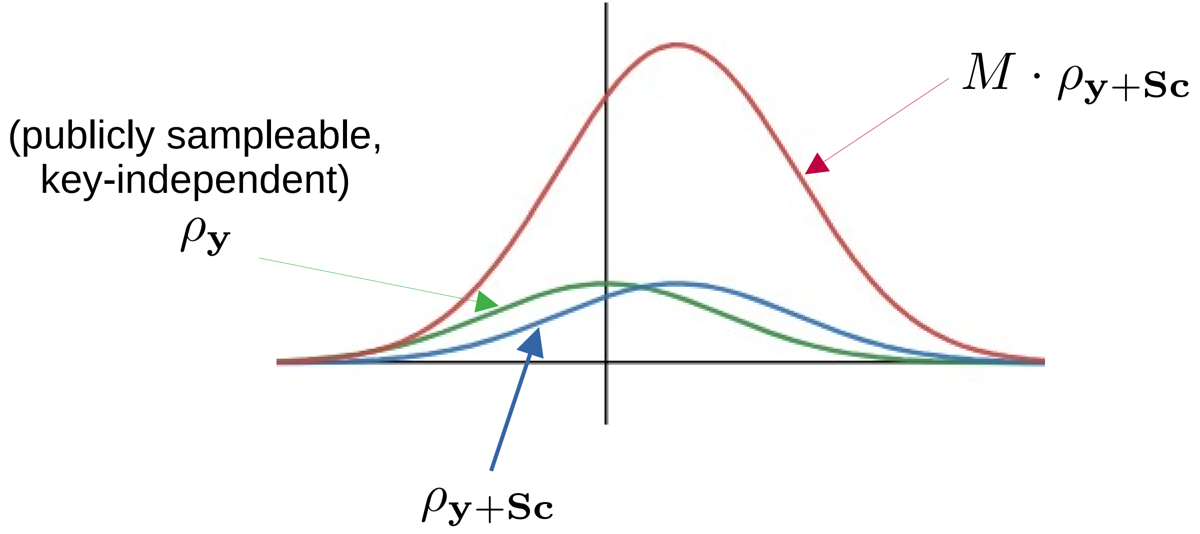
Two known approaches

Problem: we want to be able to sample from the distribution of $\mathbf{z}$ without knowing $\mathbf{S}$

$$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc}$$



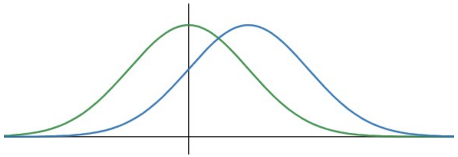
Solution 2: make the distribution of $\mathbf{z}$ independent of $\mathbf{Sc}$ by rejecting to a target distribution



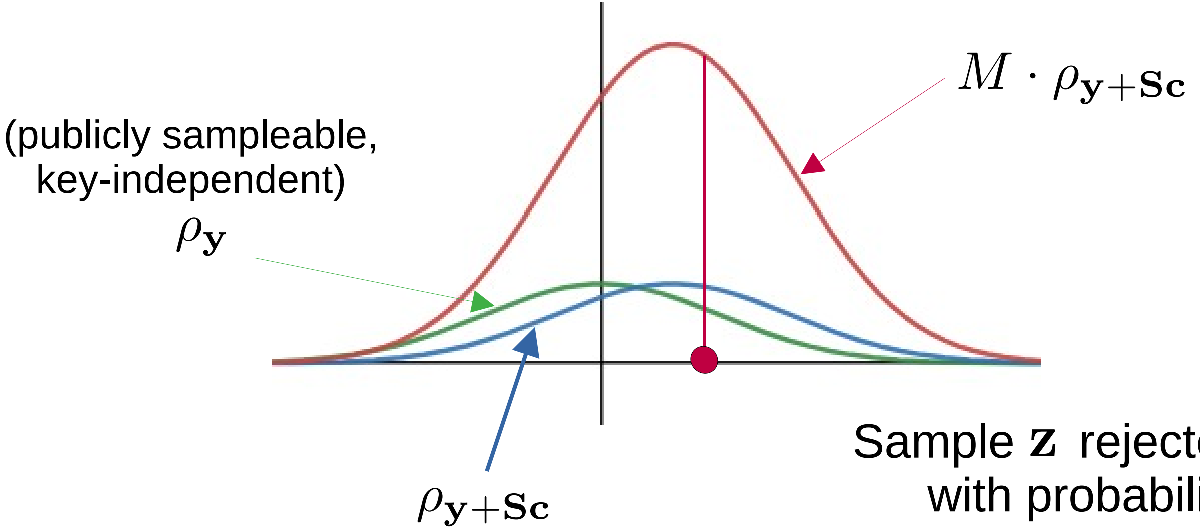
Two known approaches

Problem: we want to be able to sample from the distribution of $\mathbf{z}$ without knowing $\mathbf{S}$

$$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c}$$



Solution 2: make the distribution of $\mathbf{z}$ independent of $\mathbf{S}\mathbf{c}$ by rejecting to a target distribution

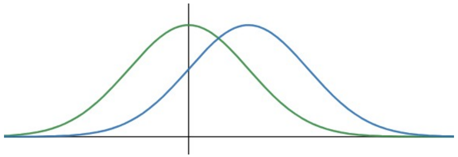


Sample $\mathbf{z}$ rejected with probability $\dfrac{\rho_{\mathbf{y}}(\mathbf{z})}{M \cdot \rho_{\mathbf{y}+\mathbf{S}\mathbf{c}}(\mathbf{z})}$

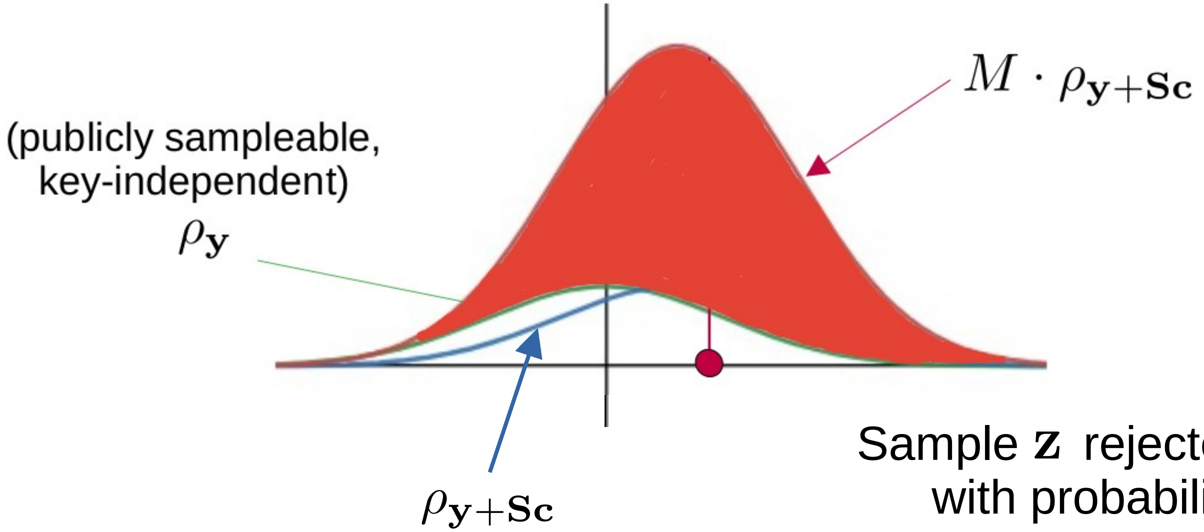
Two known approaches

Problem: we want to be able to sample from the distribution of $\mathbf{z}$ without knowing $\mathbf{S}$

$$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c}$$



Solution 2: make the distribution of $\mathbf{z}$ independent of $\mathbf{S}\mathbf{c}$ by rejecting to a target distribution

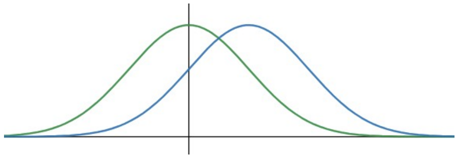


Sample $\mathbf{z}$ rejected with probability $\dfrac{\rho_{\mathbf{y}}(\mathbf{z})}{M \cdot \rho_{\mathbf{y}+\mathbf{S}\mathbf{c}}(\mathbf{z})}$

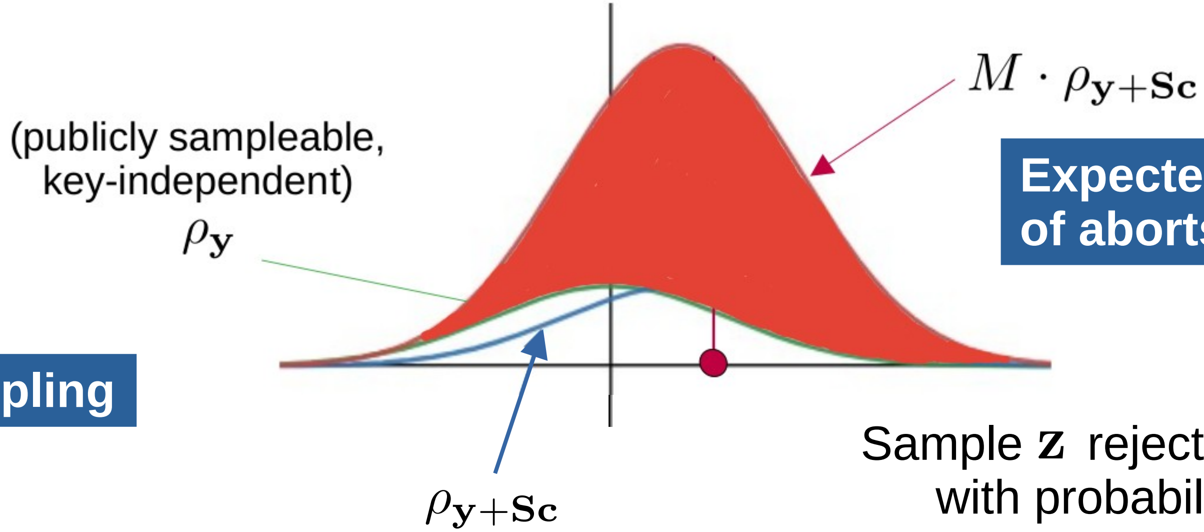
Two known approaches

Problem: we want to be able to sample from the distribution of $\mathbf{z}$ without knowing $\mathbf{S}$

$$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc}$$



Solution 2: make the distribution of $\mathbf{z}$ independent of $\mathbf{Sc}$ by rejecting to a target distribution



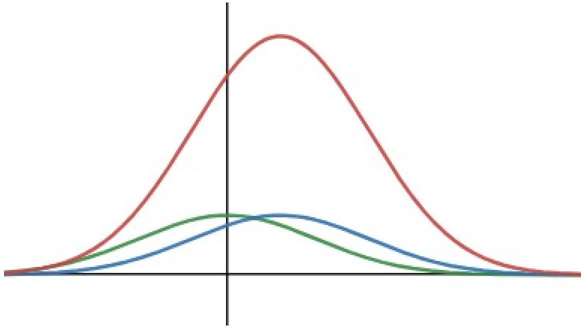
Expected number of aborts is M

Rejection sampling

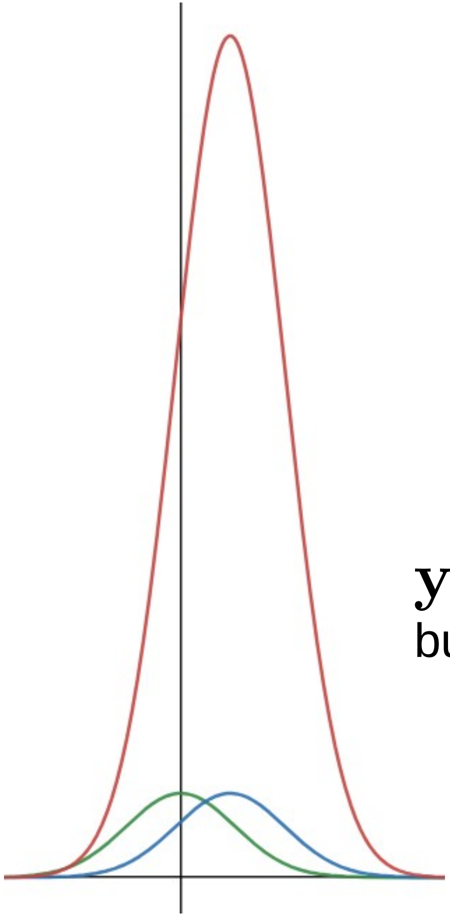
Sample $\mathbf{z}$ rejected with probability $\dfrac{\rho_{\mathbf{y}}(\mathbf{z})}{M \cdot \rho_{\mathbf{y}+\mathbf{Sc}}(\mathbf{z})}$

Trade-off: abort-rate vs size

$\mathbf{y}, \mathbf{z}$ are larger but less aborts



$\mathbf{y}, \mathbf{z}$ are smaller
but much more aborts



Using bimodal Gaussians [DDLL'13, Duc'14]

Prover

$\mathbf{A} \leftarrow \mathbb{Z}_{2q}^{m \times k}$, $\mathbf{S} \leftarrow \mathbb{Z}^{k \times \ell}$ small

$s.t.\ \mathbf{AS} = q\mathbf{I}_k \bmod 2q$

Verifier

$\mathbf{A}$

Using bimodal Gaussians [DDLL'13, Duc'14]

Prover

$\mathbf{A} \leftarrow \mathbb{Z}_{2q}^{m\times k}$, $\mathbf{S} \leftarrow \mathbb{Z}^{k\times \ell}$ small

$s.t.\ \mathbf{AS} = q\mathbf{I}_k \bmod 2q$

Verifier

$\mathbf{A}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

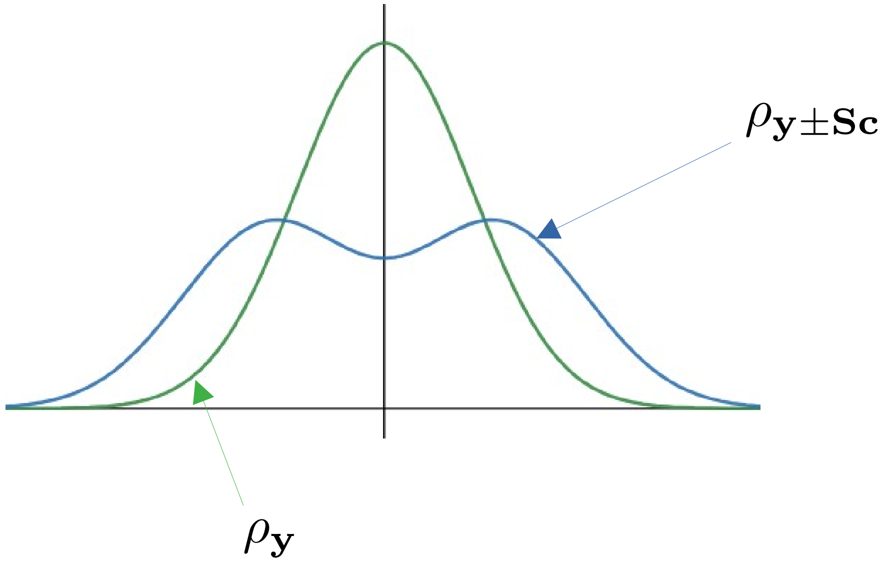
$$\boxed{\begin{array}{c} b \leftarrow U(\{0,1\}) \\ \mathbf{z} \leftarrow \mathbf{y} + (-1)^b\mathbf{Sc} \bmod 2q \end{array}} \longrightarrow$$

Verify that:

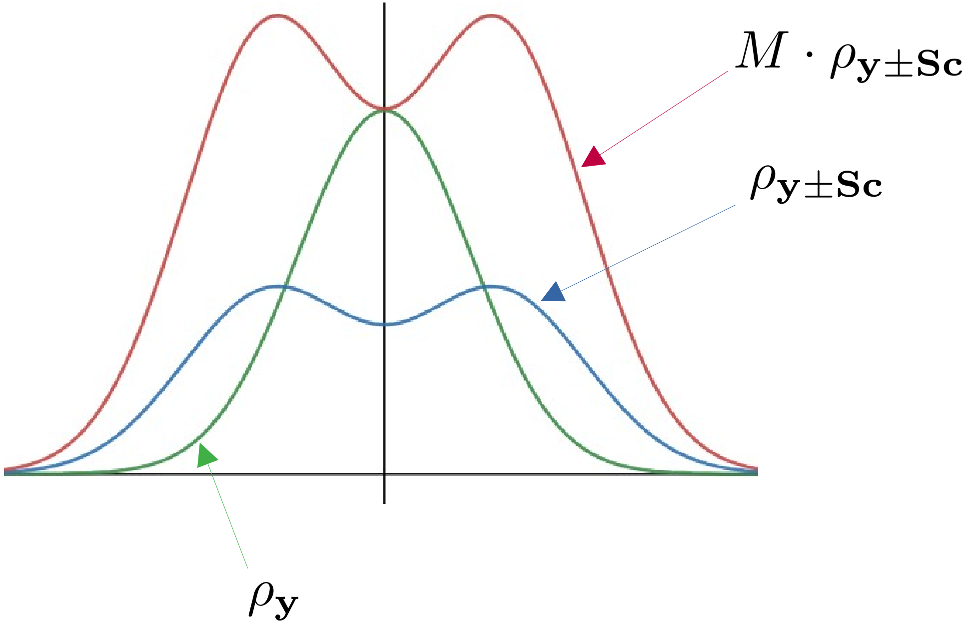
(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

Using bimodal Gaussians



Using bimodal Gaussians



The scaling factor M is much smaller… Smaller expected number of aborts.

➡ Less aborts, or reduced size for same abort-rate

Why does verification still pass?

Prover		***Verifier***
$\mathbf{A}, \mathbf{S}$ $s.t.\ \mathbf{AS} = q\mathbf{I}_k$		$\mathbf{A}$
$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$ $\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q$	$\longrightarrow$	
	$\longleftarrow$	$\mathbf{c} \leftarrow U(\{0,1\}^\ell)$
$\mathbf{z} \leftarrow \mathbf{y} \pm \mathbf{Sc} \bmod 2q$	$\longrightarrow$	Verify that: (1) $\mathbf{z}$ is small (2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

Why does verification still pass?

Prover		**Verifier**
$\mathbf{A}, \mathbf{S}$ s.t. $\mathbf{AS} = q\mathbf{I}_k$		$\mathbf{A}$
$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$ $\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q$	$\longrightarrow$	
	$\longleftarrow$	$\mathbf{c} \leftarrow U(\{0,1\}^\ell)$
$\mathbf{z} \leftarrow \mathbf{y} \pm \mathbf{Sc} \bmod 2q$	$\longrightarrow$	Verify that: (1) $\mathbf{z}$ is small (2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

$$\mathbf{AS} = q\mathbf{I}_k \bmod 2q \Rightarrow 2\mathbf{AS} = \mathbf{0} \bmod 2q$$

Why does verification still pass?

Prover | **_Verifier_**

$\mathbf{A}, \mathbf{S}$ | $\mathbf{A}$

$s.t.\ \mathbf{AS} = q\mathbf{I}_k$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} \pm \mathbf{Sc} \bmod 2q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

$$\mathbf{AS} = q\mathbf{I}_k \bmod 2q \Rightarrow 2\mathbf{AS} = \mathbf{0} \bmod 2q$$

For completeness, one needs:

$$\mathbf{Ay} + \mathbf{ASc} = \mathbf{w} + q\mathbf{c} \bmod 2q$$

Why does verification still pass?

Prover		***Verifier***
$\mathbf{A}, \mathbf{S}$ s.t. $\mathbf{AS} = q\mathbf{I}_k$		$\mathbf{A}$
$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$ $\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q$	$\longrightarrow$	
	$\longleftarrow$	$\mathbf{c} \leftarrow U(\{0,1\}^\ell)$
$\mathbf{z} \leftarrow \mathbf{y} \pm \mathbf{Sc} \bmod 2q$	$\longrightarrow$	Verify that: (1) $\mathbf{z}$ is small (2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

$$\mathbf{AS} = q\mathbf{I}_k \bmod 2q \Rightarrow 2\mathbf{AS} = \mathbf{0} \bmod 2q$$

For completeness, one needs:

$$\underbrace{\mathbf{Ay}}_{=\mathbf{w}} + \underbrace{\mathbf{AS}}_{=q\mathbf{I}_k}\mathbf{c} = \mathbf{w} + q\mathbf{c} \bmod 2q$$

Why does verification still pass?

Prover		**Verifier**
$\mathbf{A}, \mathbf{S}$ s.t. $\mathbf{AS} = q\mathbf{I}_k$		$\mathbf{A}$
$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$		
$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q$	$\longrightarrow$	
	$\longleftarrow$	$\mathbf{c} \leftarrow U(\{0,1\}^\ell)$
$\mathbf{z} \leftarrow \mathbf{y} \pm \mathbf{Sc} \bmod 2q$	$\longrightarrow$	Verify that: (1) $\mathbf{z}$ is small (2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

$$\mathbf{AS} = q\mathbf{I}_k \bmod 2q \Rightarrow 2\mathbf{AS} = \mathbf{0} \bmod 2q$$

For completeness, one needs:

$$\underbrace{\mathbf{Ay}}_{=\mathbf{w}} + \underbrace{\mathbf{ASc}}_{=q\mathbf{I}_k} = \mathbf{w} + q\mathbf{c} \bmod 2q$$

But also:

$$\mathbf{A}(\mathbf{y} - \mathbf{Sc}) = \mathbf{w} + q\mathbf{c} \bmod 2q$$

Why does verification still pass?

Prover		Verifier
$\mathbf{A}, \mathbf{S}$		$\mathbf{A}$
$s.t.\ \mathbf{AS} = q\mathbf{I}_k$		
$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$		
$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q$	$\longrightarrow$	
	$\longleftarrow$	$\mathbf{c} \leftarrow U(\{0,1\}^\ell)$
$\mathbf{z} \leftarrow \mathbf{y} \pm \mathbf{Sc} \bmod 2q$	$\longrightarrow$	Verify that:
		(1) $\mathbf{z}$ is small
		(2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

$$\mathbf{AS} = q\mathbf{I}_k \bmod 2q \Rightarrow 2\mathbf{AS} = \mathbf{0} \bmod 2q$$

For completeness, one needs:

$$\underbrace{\mathbf{Ay}}_{=\mathbf{w}} + \underbrace{\mathbf{ASc}}_{=q\mathbf{I}_k} = \mathbf{w} + q\mathbf{c} \bmod 2q$$

But also:

$$\mathbf{A}(\mathbf{y} - \mathbf{Sc}) = \mathbf{w} + q\mathbf{c} \bmod 2q$$

$$\mathbf{y} + \mathbf{Sc} - 2\mathbf{Sc}$$

Why does verification still pass?

Prover		**Verifier**
$\mathbf{A}, \mathbf{S}$ s.t. $\mathbf{AS} = q\mathbf{I}_k$		$\mathbf{A}$
$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$		
$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q$	$\longrightarrow$	
	$\longleftarrow$	$\mathbf{c} \leftarrow U(\{0,1\}^\ell)$
$\mathbf{z} \leftarrow \mathbf{y} \pm \mathbf{Sc} \bmod 2q$	$\longrightarrow$	Verify that: (1) $\mathbf{z}$ is small (2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

$$\mathbf{AS} = q\mathbf{I}_k \bmod 2q \Rightarrow 2\mathbf{AS} = \mathbf{0} \bmod 2q$$

For completeness, one needs:

$$\underbrace{\mathbf{Ay}}_{=\mathbf{w}} + \underbrace{\mathbf{ASc}}_{=q\mathbf{I}_k} = \mathbf{w} + q\mathbf{c} \bmod 2q$$

But also:

$$\mathbf{A}(\mathbf{y} - \mathbf{Sc}) = \mathbf{w} + q\mathbf{c} \bmod 2q$$
$$= \mathbf{Ay} + \mathbf{ASc} - 2\mathbf{ASc} \bmod 2q$$

$$\mathbf{y} + \mathbf{Sc} - 2\mathbf{Sc}$$

Why does verification still pass?

Prover		**Verifier**
$\mathbf{A}, \mathbf{S}$		$\mathbf{A}$
$s.t.\ \mathbf{AS} = q\mathbf{I}_k$		
$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$		
$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q$	$\longrightarrow$	
	$\longleftarrow$	$\mathbf{c} \leftarrow U(\{0,1\}^\ell)$
$\mathbf{z} \leftarrow \mathbf{y} \pm \mathbf{Sc} \bmod 2q$	$\longrightarrow$	Verify that:
		(1) $\mathbf{z}$ is small
		(2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

$$\mathbf{AS} = q\mathbf{I}_k \bmod 2q \Rightarrow 2\mathbf{AS} = \mathbf{0} \bmod 2q$$

For completeness, one needs:

$$\underbrace{\mathbf{Ay}}_{=\mathbf{w}} + \underbrace{\mathbf{ASc}}_{=q\mathbf{I}_k} = \mathbf{w} + q\mathbf{c} \bmod 2q$$

But also:

$$\mathbf{A}(\mathbf{y} - \mathbf{Sc}) = \mathbf{w} + q\mathbf{c} \bmod 2q$$
$$= \mathbf{Ay} + \mathbf{ASc} - \underbrace{2\mathbf{ASc}}_{=\mathbf{0}} \bmod 2q$$

$$\mathbf{y} + \mathbf{Sc} - 2\mathbf{Sc}$$

Why does verification still pass?

Prover		**Verifier**
$\mathbf{A}, \mathbf{S}$ s.t. $\mathbf{AS} = q\mathbf{I}_k$		$\mathbf{A}$
$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$ $\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q$	$\longrightarrow$	
	$\longleftarrow$	$\mathbf{c} \leftarrow U(\{0,1\}^\ell)$
$\mathbf{z} \leftarrow \mathbf{y} \pm \mathbf{Sc} \bmod 2q$	$\longrightarrow$	Verify that: (1) $\mathbf{z}$ is small (2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

$$\mathbf{AS} = q\mathbf{I}_k \bmod 2q \Rightarrow 2\mathbf{AS} = \mathbf{0} \bmod 2q$$

For completeness, one needs:

$$\underbrace{\mathbf{Ay}}_{=\mathbf{w}} + \underbrace{\mathbf{ASc}}_{=q\mathbf{I}_k} = \mathbf{w} + q\mathbf{c} \bmod 2q$$

But also:

$$\begin{aligned} \mathbf{A}(\mathbf{y} - \mathbf{Sc}) &= \mathbf{w} + q\mathbf{c} \bmod 2q \\ &= \mathbf{Ay} + \mathbf{ASc} - \underbrace{2\mathbf{ASc}}_{=\mathbf{0}} \bmod 2q \end{aligned}$$

Actually, for any $\mathbf{h} \in \mathbb{Z}^\ell$, we have:

$$\mathbf{A}(\mathbf{y} + \mathbf{Sc}) = \mathbf{A}(\mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh}) \bmod 2q$$

Why does verification still pass?

Prover		***Verifier***
$\mathbf{A}, \mathbf{S}$ s.t. $\mathbf{AS} = q\mathbf{I}_k$		$\mathbf{A}$
$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$		
$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q$	$\longrightarrow$	
	$\longleftarrow$	$\mathbf{c} \leftarrow U(\{0,1\}^\ell)$
$\mathbf{z} \leftarrow \mathbf{y} \pm \mathbf{Sc} \bmod 2q$	$\longrightarrow$	Verify that: (1) $\mathbf{z}$ is small (2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

$$\mathbf{AS} = q\mathbf{I}_k \bmod 2q \Rightarrow 2\mathbf{AS} = \mathbf{0} \bmod 2q$$

For completeness, one needs:

$$\underbrace{\mathbf{Ay}}_{=\mathbf{w}} + \underbrace{\mathbf{ASc}}_{=q\mathbf{I}_k} = \mathbf{w} + q\mathbf{c} \bmod 2q$$

But also:

$$\begin{aligned}\mathbf{A}(\mathbf{y} - \mathbf{Sc}) &= \mathbf{w} + q\mathbf{c} \bmod 2q \\ &= \mathbf{Ay} + \mathbf{ASc} - \underbrace{2\mathbf{ASc}}_{=\mathbf{0}} \bmod 2q\end{aligned}$$

Actually, for any $\mathbf{h} \in \mathbb{Z}^\ell$, we have:

$$\mathbf{A}(\mathbf{y} + \mathbf{Sc}) = \mathbf{A}(\mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh}) \bmod 2q$$

Any $\mathbf{z}$ of the form: $\mathbf{z} = \mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh}$ for any $\mathbf{h} \in \mathbb{Z}^\ell$ passes verification as long as it is **small**

Why does verification still pass?

Prover | **_Verifier_**

$\mathbf{A}, \mathbf{S}$ | $\mathbf{A}$

$s.t.\ \mathbf{AS} = q\mathbf{I}_k$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{z} \leftarrow \mathbf{y} \pm \mathbf{Sc} \bmod 2q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

These are our two Gaussians for G+G!

$$\mathbf{AS} = q\mathbf{I}_k \bmod 2q \Rightarrow 2\mathbf{AS} = \mathbf{0} \bmod 2q$$

mpleteness, one needs:

$$\underbrace{\mathbf{AS}}_{= q\mathbf{I}_k}\mathbf{c} = \mathbf{w} + q\mathbf{c} \bmod 2q$$

But also:

$$\mathbf{A}(\mathbf{y} - \mathbf{Sc}) = \mathbf{w} + q\mathbf{c} \bmod 2q$$
$$= \mathbf{Ay} + \mathbf{ASc} - \underbrace{2\mathbf{AS}}_{=\mathbf{0}}\mathbf{c} \bmod 2q$$

Actually, for any $\mathbf{h} \in \mathbb{Z}^\ell$, we have:

$$\mathbf{A}(\mathbf{y} + \mathbf{Sc}) = \mathbf{A}(\mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh}) \bmod 2q$$

Any $\mathbf{z}$ of the form: $\mathbf{z} = \mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh}$ for any $\mathbf{h} \in \mathbb{Z}^\ell$ passes verification as long as it is **small**

Which choice for the two Gaussians?

We set: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c} + \mathbf{2Sh} \bmod 2q$

Which choice for the two Gaussians?

We set: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} + \mathbf{2Sh} \bmod 2q$

We want the following:

1. The distribution of $\mathbf{z}$ is centered in 0

Which choice for the two Gaussians?

We set: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} + \mathbf{2Sh} \bmod 2q$

We want the following:

1. The distribution of $\mathbf{z}$ is centered in 0

$\mathbf{h} \leftarrow \mathcal{D}_{\mathbb{Z}^\ell, \sigma', \frac{-\mathbf{c}}{\mathbf{2}}}$

Which choice for the two Gaussians?

We set: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} + \mathbf{2Sh} \bmod 2q$

We want the following:

1. The distribution of $\mathbf{z}$ is centered in 0

$$\mathbf{h} \leftarrow \mathcal{D}_{\mathbb{Z}^\ell, \sigma', \frac{-\mathbf{c}}{2}} \Rightarrow 2\mathbf{Sh} \sim \mathcal{D}_{\mathbb{Z}^k, 4\sigma'^2 \mathbf{S}\mathbf{S}^\intercal, -\mathbf{Sc}}$$

Which choice for the two Gaussians?

We set: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} + \mathbf{2Sh} \bmod 2q$

We want the following:

1. The distribution of $\mathbf{Z}$ is centered in 0

$$\mathbf{h} \leftarrow \mathcal{D}_{\mathbb{Z}^\ell, \sigma', \frac{-\mathbf{c}}{2}} \Rightarrow 2\mathbf{Sh} \sim \mathcal{D}_{\mathbb{Z}^k, 4\sigma'^2 \mathbf{SS}^\intercal, -\mathbf{Sc}}$$

2. The distribution of $\mathbf{Z}$ is publicly sampleable

Which choice for the two Gaussians?

We set: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} + \mathbf{2Sh} \bmod 2q$

We want the following:

1. The distribution of $\mathbf{Z}$ is centered in 0

$$\mathbf{h} \leftarrow \mathcal{D}_{\mathbb{Z}^\ell,\sigma',\frac{-\mathbf{c}}{2}} \Rightarrow 2\mathbf{Sh} \sim \mathcal{D}_{\mathbb{Z}^k,4\sigma'^2\mathbf{SS}^\intercal,-\mathbf{Sc}}$$

2. The distribution of $\mathbf{Z}$ is publicly sampleable

$$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma^2\mathbf{I}_k-4\sigma'^2\mathbf{SS}^\intercal}$$

Which choice for the two Gaussians?

We set: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} + \mathbf{2Sh} \bmod 2q$

We want the following:

1. The distribution of $\mathbf{Z}$ is centered in 0

$$\mathbf{h} \leftarrow \mathcal{D}_{\mathbb{Z}^\ell, \sigma', \frac{-\mathbf{c}}{2}} \Rightarrow 2\mathbf{Sh} \sim \mathcal{D}_{\mathbb{Z}^k, 4\sigma'^2 \mathbf{SS}^\intercal, -\mathbf{Sc}}$$

2. The distribution of $\mathbf{Z}$ is publicly sampleable

$$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k, \sigma^2 \mathbf{I}_k - 4\sigma'^2 \mathbf{SS}^\intercal} \Rightarrow \mathbf{z} \sim \mathcal{D}_{\mathbb{Z}^k, \sigma}$$

Which choice for the two Gaussians?

We set: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} + \mathbf{2Sh} \bmod 2q$

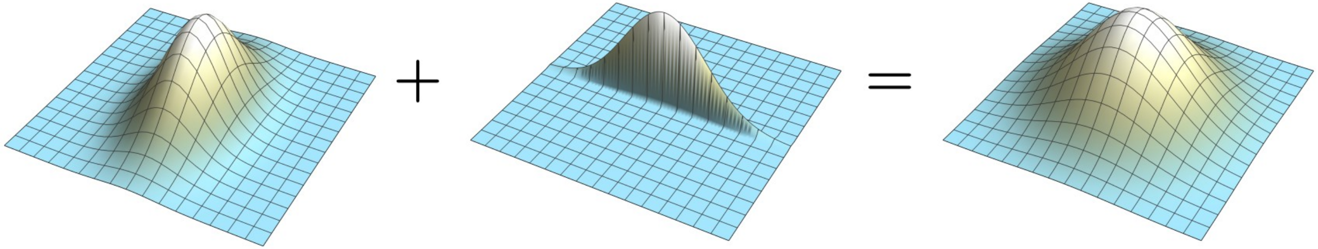
We want the following:

1. The distribution of $\mathbf{z}$ is centered in 0

$$\mathbf{h} \leftarrow \mathcal{D}_{\mathbb{Z}^\ell, \sigma', \frac{-\mathbf{c}}{2}} \Rightarrow 2\mathbf{Sh} \sim \mathcal{D}_{\mathbb{Z}^k, 4\sigma'^2 \mathbf{SS}^\intercal, -\mathbf{Sc}}$$

2. The distribution of $\mathbf{z}$ is publicly sampleable

$$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k, \sigma^2 \mathbf{I}_k - 4\sigma'^2 \mathbf{SS}^\intercal} \Rightarrow \mathbf{z} \sim \mathcal{D}_{\mathbb{Z}^k, \sigma}$$



Which choice for the two Gaussians?

We set: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} + \mathbf{2Sh} \bmod 2q$

We want the following:

1. The distribution of $\mathbf{z}$ is centered in 0

$$\mathbf{h} \leftarrow \mathcal{D}_{\mathbb{Z}^\ell, \sigma', \frac{-\mathbf{c}}{2}} \Rightarrow \mathbf{2Sh} \sim \mathcal{D}_{\mathbb{Z}^k, 4\sigma'^2\mathbf{SS}^\intercal, -\mathbf{Sc}}$$

2. The distribution of $\mathbf{z}$ is publicly sampleable

$$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k, \sigma^2\mathbf{I}_k - 4\sigma'^2\mathbf{SS}^\intercal} \Rightarrow \mathbf{z} \sim \mathcal{D}_{\mathbb{Z}^k, \sigma}$$

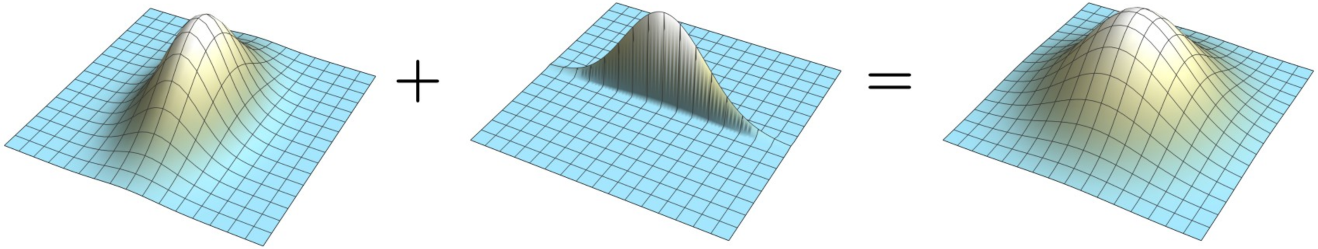
[BMKMS'22,GMPW'20]

We are actually interested in the discrete case but we can make it work as well. Assuming:

$$\sigma' \geq \sqrt{2\ln(\ell - 1 + 2\ell/\epsilon)/\pi}$$
$$\sigma \geq \sqrt{8} \cdot \sigma_1(\mathbf{S}) \cdot \sigma'$$

Then:

$$\mathbf{z} \sim_\epsilon \mathcal{D}_{\mathbb{Z}^k, \sigma}$$



The G+G protocol

Prover | ***Verifier***

$\mathbf{A} \leftarrow \mathbb{Z}_{2q}^{m\times k}, \mathbf{S} \leftarrow \mathbb{Z}^{k\times \ell}$ **small**

$s.t.\ \mathbf{A}\mathbf{S} = q\mathbf{I}_k \bmod 2q$

$\mathbf{A}$

The G+G protocol

Prover | **Verifier**

$\mathbf{A} \leftarrow \mathbb{Z}_{2q}^{m\times k}$, $\mathbf{S} \leftarrow \mathbb{Z}^{k\times \ell}$ small | $\mathbf{A}$

$s.t.\ \mathbf{AS} = q\mathbf{I}_k \bmod 2q$

$$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k, \sigma^2\mathbf{I}_k - 4\sigma'^2\mathbf{S}\mathbf{S}^\intercal}$$

$$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q \longrightarrow$$

The G+G protocol

Prover | **Verifier**

$\mathbf{A} \leftarrow \mathbb{Z}_{2q}^{m\times k}$, $\mathbf{S} \leftarrow \mathbb{Z}^{k\times \ell}$ small

$s.t.\ \mathbf{AS} = q\mathbf{I}_k \bmod 2q$

Verifier: $\mathbf{A}$

$$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k, \sigma^2\mathbf{I}_k - 4\sigma'^2\mathbf{S}\mathbf{S}^\intercal}$$

$$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q \longrightarrow$$

$$\longleftarrow \quad \mathbf{c} \leftarrow U(\{0,1\}^\ell)$$

The G+G protocol

Prover | ***Verifier***

$\mathbf{A} \leftarrow \mathbb{Z}_{2q}^{m\times k}, \mathbf{S} \leftarrow \mathbb{Z}^{k\times \ell}$ small | $\mathbf{A}$

$s.t.\ \mathbf{AS} = q\mathbf{I}_k \bmod 2q$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k, \sigma^2\mathbf{I}_k - 4\sigma'^2\mathbf{S}\mathbf{S}^\intercal}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{y} \bmod 2q$ $\longrightarrow$

$\longleftarrow$ $\mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{h} \leftarrow \mathcal{D}_{\mathbb{Z}^\ell, \sigma', -\mathbf{c}/2}$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c} + 2\mathbf{S}\mathbf{h} \bmod 2q$ $\longrightarrow$

The G+G protocol

Prover

Verifier

$\mathbf{A} \leftarrow \mathbb{Z}_{2q}^{m\times k}$, $\mathbf{S} \leftarrow \mathbb{Z}^{k\times \ell}$ small

$s.t.\ \mathbf{AS} = q\mathbf{I}_k \bmod 2q$

$\mathbf{A}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k, \sigma^2 \mathbf{I}_k - 4\sigma'^2 \mathbf{S}\mathbf{S}^\intercal}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{h} \leftarrow \mathcal{D}_{\mathbb{Z}^\ell, \sigma', -\mathbf{c}/2}$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh} \bmod 2q \longrightarrow$

Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

Properties of G+G

Prover	*Verifier*
$\mathbf{A}, \mathbf{S}$ $s.t.\ \mathbf{AS} = q\mathbf{I}_k$	$\mathbf{A}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k, \sigma^2 \mathbf{I}_k - 4\sigma'^2 \mathbf{S}\mathbf{S}^\intercal}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{h} \leftarrow \mathcal{D}_{\mathbb{Z}^\ell, \sigma', -\mathbf{c}/2}$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh} \bmod 2q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

Properties of G+G

Prover

$\mathbf{A}, \mathbf{S}$

$s.t.\ \mathbf{AS} = q\mathbf{I}_k$

Verifier

$\mathbf{A}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k, \sigma^2 \mathbf{I}_k - 4\sigma'^2 \mathbf{S}\mathbf{S}^\intercal}$

$\mathbf{w} \leftarrow \mathbf{A}\mathbf{y} \bmod 2q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{h} \leftarrow \mathcal{D}_{\mathbb{Z}^\ell, \sigma', -\mathbf{c}/2}$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c} + 2\mathbf{S}\mathbf{h} \bmod 2q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

<u>Completeness:</u>

$$\mathbf{Az} = \mathbf{A}(\mathbf{y} + \mathbf{Sc} + \mathbf{2Sh}) = \mathbf{w} + q\mathbf{c} \bmod 2q$$

$\mathbf{z} = \mathbf{y} + \mathbf{Sc} + \mathbf{2Sh}$ is small

<u>Soundness:</u>

From the hardness of SIS (or LWE)

Properties of G+G

Prover

$\mathbf{A}, \mathbf{S}$

$s.t.\ \mathbf{AS} = q\mathbf{I}_k$

Verifier

$\mathbf{A}$

$\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^k, \sigma^2\mathbf{I}_k - 4\sigma'^2\mathbf{S}\mathbf{S}^\intercal}$

$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q \longrightarrow$

$\longleftarrow \mathbf{c} \leftarrow U(\{0,1\}^\ell)$

$\mathbf{h} \leftarrow \mathcal{D}_{\mathbb{Z}^\ell, \sigma', -\mathbf{c}/2}$

$\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh} \bmod 2q \longrightarrow$ Verify that:

(1) $\mathbf{z}$ is small

(2) $\mathbf{Az} = \mathbf{w} + q\mathbf{c} \bmod 2q$

Completeness:

$$\mathbf{Az} = \mathbf{A}(\mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh}) = \mathbf{w} + q\mathbf{c} \bmod 2q$$

$\mathbf{z} = \mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh}$ is small

Soundness:

From the hardness of SIS (or LWE)

Zero-knowledge:

Simulator simply does the following:

$$\mathbf{z} \leftarrow \mathcal{D}_{\mathbb{Z}^k, \sigma}$$
$$\mathbf{w} \leftarrow \mathbf{Az} - q\mathbf{c} \bmod 2q$$

Performances of the resulting Fiat-Shamir signature

		Signature size (kB)			Public-key size (kB)		
	Security	120-bit	180-bit	260-bit	120-bit	180-bit	260-bit
(flooding)	Raccoon	12	14	20.5	2.3	3.2	4.1
(aborts, unimodal, hypercubes)	Dilithium	2.4	3.3	4.6	1.3	1.9	2.6
(aborts, unimodal, hyperballs)	DF**P**S22	1.9	2.5	3.4	0.8	1.1	1.8
(aborts, bimodal, hyperballs)	HAETAE	1.5	2.3	2.9	1.0	1.5	2.1
(convolved Gaussians)	**G+G**	**1.7**	**2.1**	**2.8**	**1.5**	**1.9**	**2.3**

Performances of the resulting Fiat-Shamir signature

		Signature size (kB)			Public-key size (kB)		
	Security	120-bit	180-bit	260-bit	120-bit	180-bit	260-bit
(flooding)	Raccoon	12	14	20.5	2.3	3.2	4.1
(aborts, unimodal, hypercubes)	Dilithium	2.4	3.3	4.6	1.3	1.9	2.6
(aborts, unimodal, hyperballs)	DF**P**S22	1.9	2.5	3.4	0.8	1.1	1.8
(aborts, bimodal, hyperballs)	HAETAE	1.5	2.3	2.9	1.0	1.5	2.1
(convolved Gaussians)	**G+G**	**1.7**	**2.1**	**2.8**	**1.5**	**1.9**	**2.3**

Performances of the resulting Fiat-Shamir signature

		Signature size (kB)			Public-key size (kB)		
	Security	120-bit	180-bit	260-bit	120-bit	180-bit	260-bit
(flooding)	Raccoon	12	14	20.5	2.3	3.2	4.1
(aborts, unimodal, hypercubes)	Dilithium	2.4	3.3	4.6	1.3	1.9	2.6
(aborts, unimodal, hyperballs)	DF**P**S22	1.9	2.5	3.4	0.8	1.1	1.8
(aborts, bimodal, hyperballs)	HAETAE	1.5	2.3	2.9	1.0	1.5	2.1
(convolved Gaussians)	**G+G**	**1.7**	**2.1**	**2.8**	**1.5**	**1.9**	**2.3**

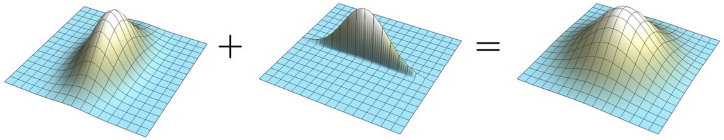
Conclusion

More in the paper:

- Detailed analysis (SD and RD) in the ROM and QROM
- Parameters (asymptotic and concrete)
- Optimizations
- NTRU instantiation

Open problems:

- Extension to ZK proofs
- Extension to advanced signatures (e.g., threshold signatures)



Thanks! eprint/2023/1477