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

ePrint 2023/1477 (Update soon!)

Julien Devevey[1], Alain Passelègue[1,2,3] and Damien Stehlé[1,3]

Oct. 18, 2023

1. École Normale Supérieure de Lyon
2. INRIA
3. CryptoLab, France

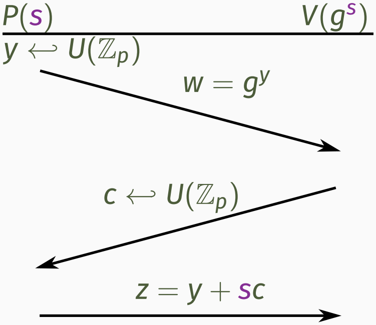
A Brief Overview

- New adapation of Schnorr's Σ-protocol for lattices

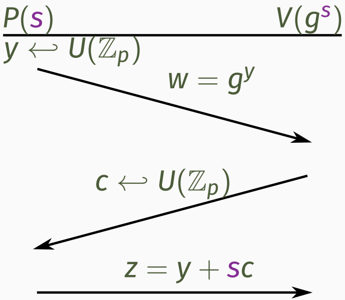
Based on	Rejection Sampling	Flooding	Convolution
Sizes	Small	Big	Small(er)
Aborts	Yes	No	No
Signature	Dilithium, HAETAE	Raccoon	G+G

Schnorr's Protocol: a Σ-protocol for Discrete Log

Schnorr's Protocol

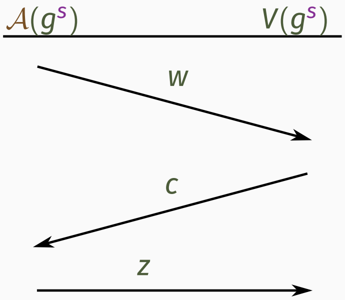


Properties



- **Completeness**: $V(g^s)$ accepts if $g^z = g^y(g^s)^c$

Properties

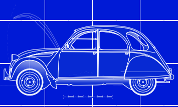


- Completeness: $V(g^s)$ accepts if $g^z = g^y(g^s)^c$
- Soundness: $V(g^s)$ rejects after interacting with $\mathcal{A}(g^s)$ under the DLog assumption

Properties

$\mathrm{Sim}(g^s) \approx (w, c, z)$

$z \hookleftarrow U(\mathbb{Z}_p)$
$c \hookleftarrow U(\mathcal{C})$
$w = g^z (g^s)^{-c}$
Return (w, c, z)



- Completeness: $V(g^s)$ accepts if $g^z = g^y (g^s)^c$
- Soundness: $V(g^s)$ rejects after interacting with $\mathcal{A}(g^s)$ under the DLog assumption
- HVZK: Nothing is revealed on s

The Fiat-Shamir Transform [FS86]

Sign(s, μ):

1: $y \hookleftarrow U(\mathbb{Z}_p)$

2: $w \leftarrow g^y$

3: $c = H(w, \mu)$

4: $z = y + cs$

5: Output $\sigma = (c, z)$

Verify(g^s, μ, σ):

1: $w = g^z (g^s)^{-c}$

2: Check that $c = H(w, \mu)$

The Fiat-Shamir Transform [FS86]

Sign(s, μ):

1: $y \hookleftarrow U(\mathbb{Z}_p)$
2: $w \leftarrow g^y$
3: $c = H(w, \mu)$
4: $z = y + cs$
5: Output $\sigma = (c, z)$

Verify(g^s, μ, σ):

1: $w = g^z (g^s)^{-c}$
2: Check that $c = H(w, \mu)$

Properties:

- Completeness implies correctness
- Soundness implies EU-NMA

(Attacks without signing queries)

- Add HVZK to get EU-CMA

(Simulate the Sign *oracle to make it useless)*

Expression in the Lattice Setting

Schnorr's Protocol: a Σ-protocol for Discrete Log

Expression in the Lattice Setting

The G+G Protocol

Learning with Errors $\mathsf{LWE}_{m,k,q,\chi}$

Given $\mathbf{A}_0 \hookleftarrow U(\mathbb{Z}_q^{m\times(k-m)})$, $\mathbf{A} = (\mathbf{A}_0|\mathbf{I}_m)$ and $\mathbf{t} \in \mathbb{Z}_q^m$, find if $\mathbf{t} \hookleftarrow U(\mathbb{Z}_q^m)$ or if $\mathbf{t} = \mathbf{A}\mathbf{s}$ for short $\mathbf{s} \hookleftarrow \chi^k$

Lattice-based Assumptions

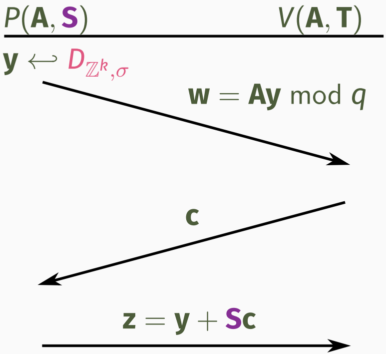
Learning with Errors $\mathsf{LWE}_{m,k,q,\chi}$

Given $\mathbf{A}_0 \hookleftarrow U(\mathbb{Z}_q^{m\times(k-m)})$, $\mathbf{A} = (\mathbf{A}_0|\mathbf{I}_m)$ and $\mathbf{t} \in \mathbb{Z}_q^m$, find if $\mathbf{t} \hookleftarrow U(\mathbb{Z}_q^m)$ or if $\mathbf{t} = \mathbf{As}$ for short $\mathbf{s} \hookleftarrow \chi^k$

Short Integer Solution $\mathsf{SIS}_{m,k,\gamma}$

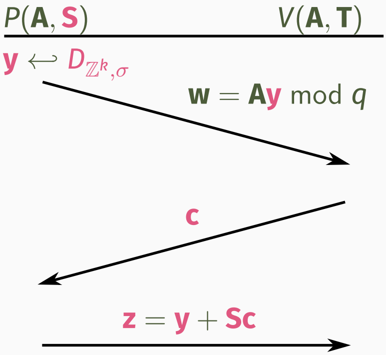
Given $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times k})$, find $\mathbf{x} \in \mathbb{Z}^k$ such that $\|\mathbf{x}\| \leq \gamma$ and $\mathbf{Ax} = 0 \bmod q$

Lyubashevsky's Protocol [Lyu09,Lyu12]



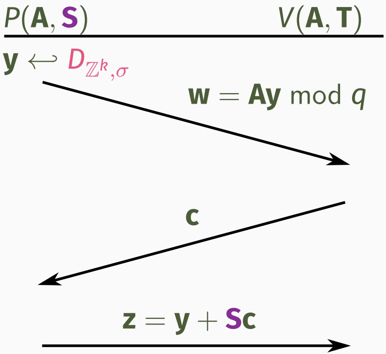
- $\mathbf{AS} = \mathbf{T} \bmod q$ and $\mathbf{S}$ is short
- Short $\mathbf{y}$ sampled from $D_{\mathbb{Z}^k,\sigma}$
- $\mathbf{c}$ is binary

Lyubashevsky's Protocol [Lyu09,Lyu12]



- $\mathbf{A}\mathbf{S} = \mathbf{T} \bmod q$ and $\mathbf{S}$ is short
- $\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c}$ is small
- $\mathbf{A}\mathbf{z} = \mathbf{A}\mathbf{y} + \mathbf{A}\mathbf{S}\mathbf{c} = \mathbf{w} + \mathbf{T}\mathbf{c} \bmod q$
- V checks $\|\mathbf{z}\| \leq \gamma$ and $\mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c} = \mathbf{w} \bmod q$

Lyubashevsky's Protocol [Lyu09,Lyu12]



- $\mathbf{AS} = \mathbf{T} \bmod q$ and $\mathbf{S}$ is short
- V checks $\|\mathbf{z}\| \leq \gamma$ and $\mathbf{Az} - \mathbf{Tc} = \mathbf{w} \bmod q$
- The protocol is complete
- Soundness based on SIS

HVZK for Lyubashevsky's Protocol

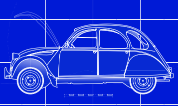
$\mathsf{Sim}(\mathbf{A}, \mathbf{T}) \approx (\mathbf{w}, \mathbf{c}, \mathbf{z})$

$\mathbf{z} \hookleftarrow ???$

$\mathbf{c} \hookleftarrow U(\mathcal{C})$

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

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

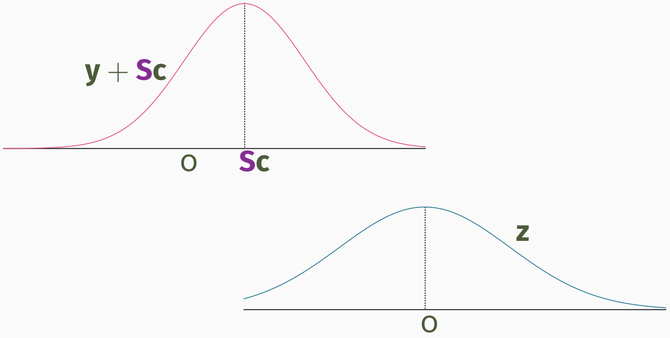


- $\mathbf{z} \hookleftarrow P$ where P is independent of $\mathbf{S}$
- $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$ actually leaks $\mathbf{Sc}$
- Key recovery attacks

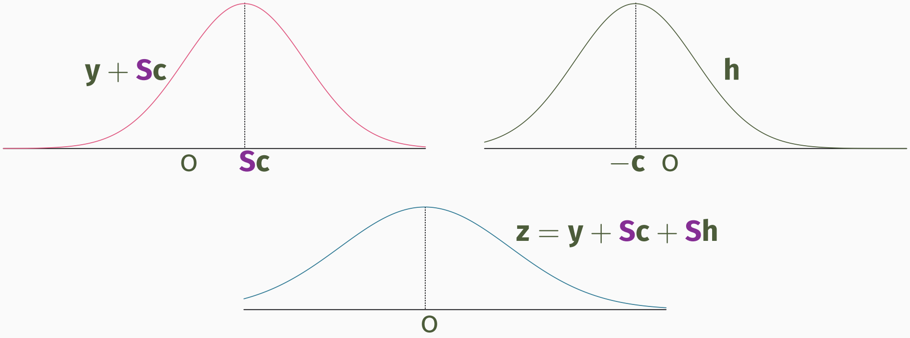
$\Longrightarrow$ Introduction of rejection sampling and flooding

The G+G Protocol

Erasing the Center



Erasing the Center



New problem: $\mathbf{Az} - \mathbf{Tc} = \mathbf{Ay} + \mathbf{Th} \bmod q$. How to make the scheme correct?

More Solutions, More Problems

Changing the Key Generation

Problem: $\mathbf{Th} = 0 \bmod q$

Solution: Take $\mathbf{AS} = 0 \bmod q$

More Solutions, More Problems

Changing the Key Generation

Problem: $\mathbf{Th} = 0 \bmod q$

Solution: Take $\mathbf{AS} = 0 \bmod q$

Problem: $\mathbf{Sc}$ can be omitted from $\mathbf{z}$ as $\mathbf{Az} = \mathbf{Ay} \bmod q$

More Solutions, More Problems

Changing the Key Generation

Problem: $\mathbf{Th} = 0 \bmod q$

Solution: Take $\mathbf{AS} = 0 \bmod q$

Problem: $\mathbf{Sc}$ can be omitted from $\mathbf{z}$ as $\mathbf{Az} = \mathbf{Ay} \bmod q$

Solution: Use $2q$ and $2\mathbf{AS} = 0 \bmod 2q$ while $\mathbf{AS} \neq 0 \bmod 2q$

Sample $\mathbf{h}$ centered around $-\mathbf{c}/2$ and set $\mathbf{z} = \mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh}$

More Solutions, More Problems

Changing the Key Generation

Problem: $\mathbf{Th} = 0 \bmod q$

Solution: Take $\mathbf{AS} = 0 \bmod q$

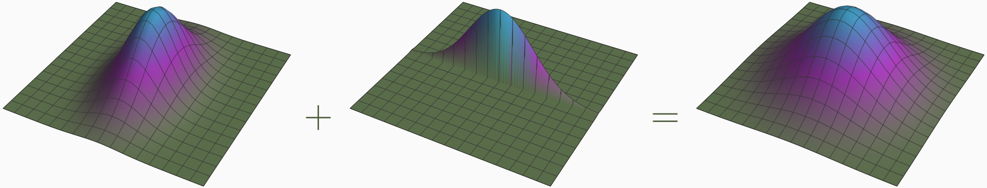
Problem: $\mathbf{Sc}$ can be omitted from $\mathbf{z}$ as $\mathbf{Az} = \mathbf{Ay} \bmod q$

Solution: Use $2q$ and $2\mathbf{AS} = 0 \bmod 2q$ while $\mathbf{AS} \neq 0 \bmod 2q$

Sample $\mathbf{h}$ centered around $-\mathbf{c}/2$ and set $\mathbf{z} = \mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh}$

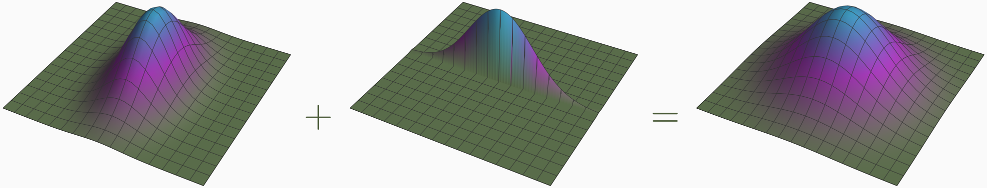
Final Problem: What is the final distribution of $\mathbf{z} = \mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh}$?

Gaussian Convolution (Continuous Case)



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

Gaussian Convolution (Continuous Case)



$\mathbf{y}$ $\quad$ $\mathbf{Sc} + 2\mathbf{Sh}$ $\quad$ $\mathbf{z}$

$\mathrm{var}(\mathbf{y})$ $\quad$ $\mathrm{var}(\mathbf{Sc} + 2\mathbf{Sh})$ $\quad$ $\mathrm{var}(\mathbf{z})$

Discrete Gaussian Case

Set $\Sigma(\mathbf{S}) = \sigma^2 \mathbf{I}_k - 4s^2 \mathbf{S}\mathbf{S}^\top$.

Sample $\mathbf{y} \hookleftarrow D_{\mathbb{Z}^k, \Sigma(\mathbf{S})}$ and $\mathbf{h} \hookleftarrow D_{\mathbb{Z}^n, s, -\mathbf{c}/2}$.

- $\sigma \geq \sqrt{8}\sigma_1(\mathbf{S}) \cdot s$

(Positive definite)

Discrete Gaussian Case

Set $\Sigma(\mathbf{S}) = \sigma^2 \mathbf{I}_k - 4s^2 \mathbf{S}\mathbf{S}^\top$.
Sample $\mathbf{y} \hookleftarrow D_{\mathbb{Z}^k, \Sigma(\mathbf{S})}$ and $\mathbf{h} \hookleftarrow D_{\mathbb{Z}^n, s, -\mathbf{c}/2}$.
Set $\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c} + 2\mathbf{S}\mathbf{h}$.

- $\sigma \geq \sqrt{8}\sigma_1(\mathbf{S}) \cdot s$
(Positive definite)
- $s \geq \sqrt{2\ln(d - 1 + 2d/\varepsilon)/\pi}$
(Smoothing quality)

Quality

$$P_{\mathbf{z}} \approx_\varepsilon D_{\mathbb{Z}^k, \sigma}$$

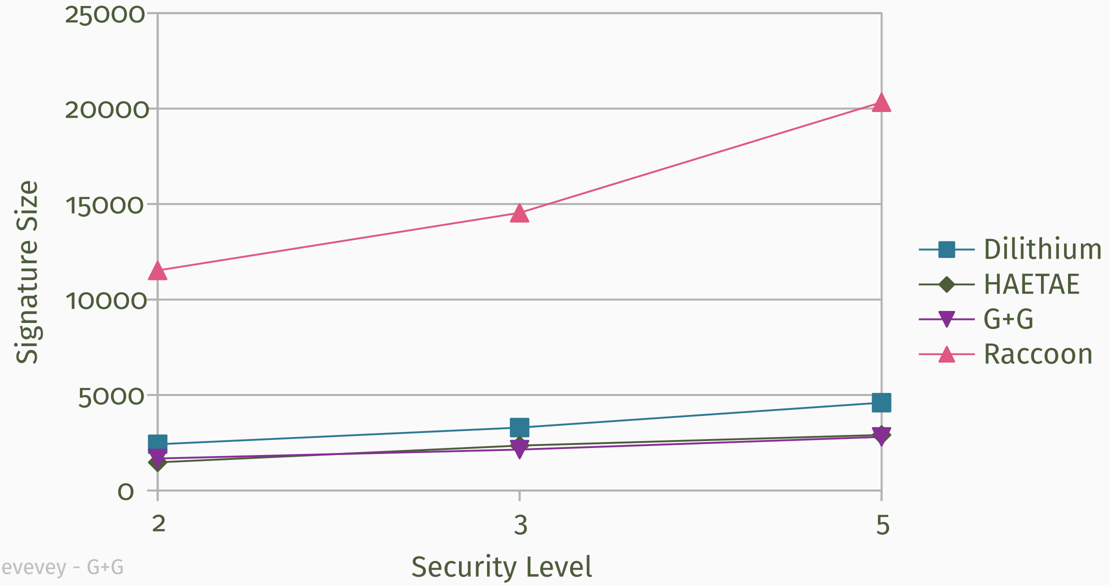
The G+G Scheme

$\mathsf{P}(\mathbf{A}, \mathbf{S})$		$\mathsf{V}(\mathbf{A}, \mathbf{T} = \mathbf{AS})$
$\mathbf{y} \hookleftarrow D_{\mathbb{Z}^k, \Sigma(\mathbf{S})}$		
$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q$	$\xrightarrow{\mathbf{w}}$	
	$\xleftarrow{\mathbf{c}}$	$\mathbf{c} \hookleftarrow U(\mathcal{C})$
$\mathbf{h} \hookleftarrow D_{\mathbb{Z}^n, s, -\mathbf{c}/2}$		
$\mathbf{z} \leftarrow \mathbf{y} + 2\mathbf{Sh} + \mathbf{Sc} \bmod 2q$	$\xrightarrow{\mathbf{z}}$	Accept if
		$\mathbf{Az} = \mathbf{w} + \mathbf{Tc} \bmod 2q$
		and $\|\mathbf{z}\| \leq \gamma$

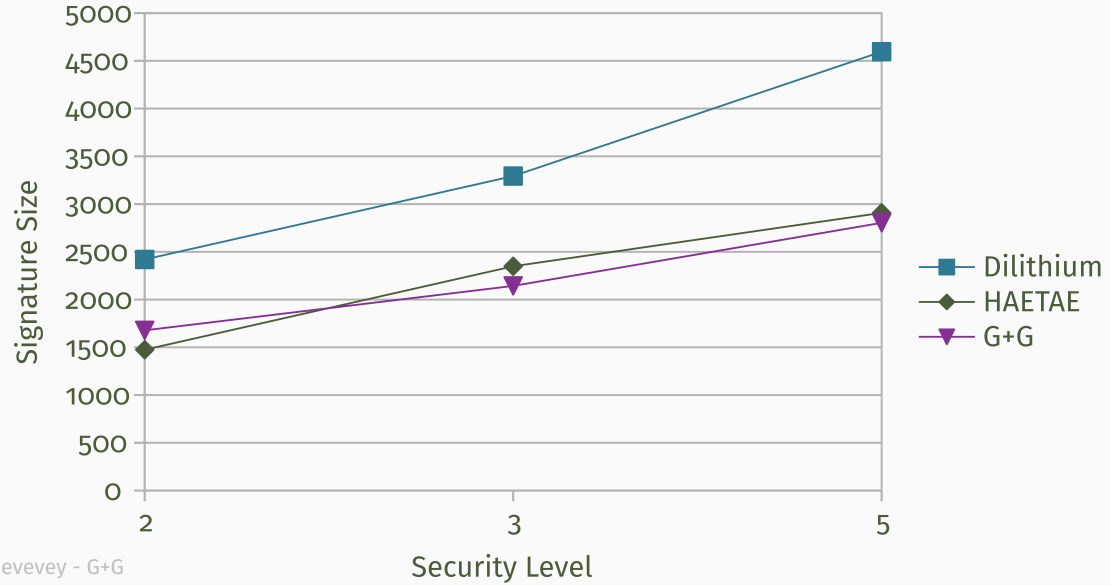
Properties

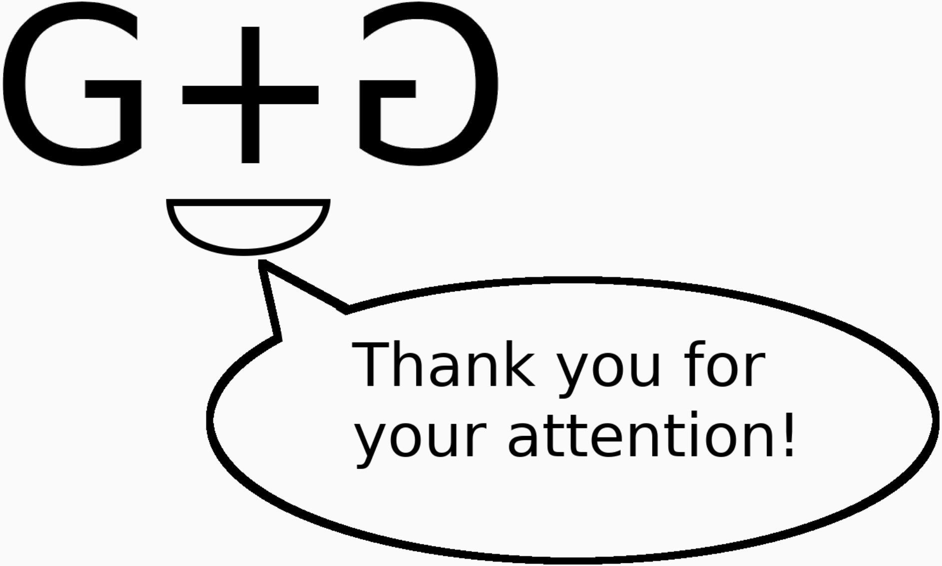
- Completeness: $\mathbf{Az} - \mathbf{Tc} = \mathbf{Ay} + (\mathbf{AS} - \mathbf{T})\mathbf{c} + 2\mathbf{ASh} = \mathbf{Ay} = \mathbf{w} \bmod 2q$
- Soundness: Based on SIS, as before
- HVZK: Sample $\mathbf{z} \hookleftarrow D_{\mathbb{Z}^k,\sigma}$ and $\mathbf{c} \hookleftarrow U(\mathcal{C})$. Set $\mathbf{w} = \mathbf{Az} - \mathbf{Tc} \bmod 2q$

Comparison with other Signatures



Comparison with other Signatures




Thank you for your attention!