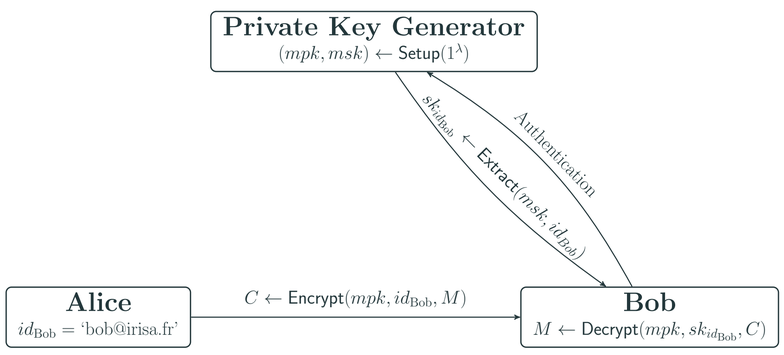
Practical Implementation of Ring-SIS/LWE based Signature and IBE

Pauline Bert, Pierre-Alain Fouque, Adeline Roux-Langlois, and Mohamed Sabt

Identity Based Encryption



1984 Concept introduced by Shamir,

2001 First realizations based on bilinear maps (by Boneh and Franklin) and on quadratic residue assumptions (by Cocks),

2008 First lattice based IBE, by Gentry, Peikert, and Vaikuntanathan,

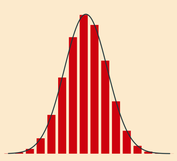
2017 First code based IBE, by Gaborit, Hauteville, Phan and Tillich.

→ **Advantages:** we no longer need certificates, PKI, cross-certification, revocation lists etc.

Learning With Errors Problem (LWE) [Reg05]

Given $\left(\mathbf{A}, \mathbf{s}\mathbf{A} + \mathbf{e} \bmod q\right)$, where

- $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{n\times m})$,
- $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$,
- $\mathbf{e} \hookleftarrow D_{\mathbb{Z}^m,\alpha q}$.



⋆ **Computational problem:** Find $\mathbf{s}$.

⋆ **Decisional problem:** Distinguish from $\left(\mathbf{A}, \mathbf{b}\right)$ with $\mathbf{b} \hookleftarrow U(\mathbb{Z}_q^m)$.

→ **Hardness:** Regev gave a reduction from **worst-case** problems on lattices to the **average-case** LWE problem.

Leftover Hash Lemma

Let q prime, and $m \geq 2n \log q$, then

$$\begin{cases} \mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{n\times m}) \\ \mathbf{x} \hookleftarrow D_{\mathbb{Z}^m,\sigma} \text{ with } \sigma \geq \omega(\sqrt{\log m}) \end{cases}$$

$$\Rightarrow \mathbf{u} = \mathbf{A}\mathbf{x} \mod q \approx_s U(\mathbb{Z}_q^n)$$

Gaussian tailcut

$$\Pr_{\mathbf{x}\hookleftarrow D_{\mathbb{Z},\sigma}}[|x| > \omega(t\sigma)] \leq 2^{-\omega(t^2)}$$

$\Rightarrow \mathbf{x} \hookleftarrow D_{\mathbb{Z}^m,\sigma}$ would have norm $\|\mathbf{x}\| \leq t\sigma\sqrt{m}$ with overwhelming probability.

Inhomogeneous Short Integer Solution Problem (ISIS) [Ajt96]

Given an uniformly random matrix $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{n\times m})$, find a non trivial **short** vector $\mathbf{x} \in \mathbb{Z}^m$ such that $\|\mathbf{x}\| \leq \beta$ and:

$$\mathbf{A}\,\mathbf{x} = \mathbf{u} \mod q.$$

→ **Hardness:** Ajtai gave a reduction from **worst-case** problems on lattices to the **average-case** SIS problem.

Trapdoor [Ajt96; MP12]

We can generate a public $\mathbf{A}$ together with a **trapdoor** $\mathbf{T}$

$(\mathbf{A}, \mathbf{T}) \leftarrow \mathsf{TrapGen}(\mathbf{H})$

We use $\mathbf{T}$ to **solve the ISIS problem**, find $\mathbf{x}$ Gaussian of parameter ζ satisfying $\mathbf{A}\mathbf{x} = \mathbf{u} \mod q$:

$\mathbf{x} \leftarrow \mathsf{SamplePre}(\mathbf{R}, \mathbf{A}, \mathbf{H}, \zeta, \mathbf{u})$

FRD map [ABB10]

$H : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n\times n}$ is an encoding with Full-Rank Differences if:

- for all $u \in \mathbb{Z}_q^n$ the matrix $H(u)$ is invertible,
- for all distinct $u, v \in \mathbb{Z}_q^n$, $H(u) - H(v)$ is full rank.

$\mathsf{TrapGen}(\mathbf{H})$:

$\mathbf{A}' \hookleftarrow U\left(\mathbb{Z}_q^{n\times(m-nk)}\right)$
$\mathbf{T} \hookleftarrow D_{\mathbb{Z}^{(m-nk)\times nk},\sigma}$
$\mathbf{A} = \left(\mathbf{A}' \,|\, \mathbf{H}\mathbf{G} - \mathbf{A}'\mathbf{T}\right)$
return $(\mathbf{A}, \mathbf{T})$

where $k = \lceil \log_2 q \rceil$, and

- $\mathbf{G} \in \mathbb{Z}_q^{n\times nk}$ a public **'gadget'** with a structured basis,
- $\mathbf{H} \in \mathbb{Z}_q^{n\times n}$ invertible.

Dual-Regev Public Key Encryption scheme [GPV08]

$\mathsf{Keygen}(1^\lambda)$:

$\mathbf{x} \hookleftarrow D_{\mathbb{Z}^m,\zeta}$
$\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{n\times m})$
return $pk = (\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x} \mod q)$ and $vk = \mathbf{x}$

$\mathsf{Encrypt}(pk, M \in \{0,1\})$:

$\mathbf{e} \hookleftarrow D_{\mathbb{Z}^m,\alpha q}$, and $e' \hookleftarrow D_{\mathbb{Z},\alpha q}$
$\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$
$\mathbf{c}_0^T = \mathbf{s}^T\mathbf{A} + \mathbf{e}^T$
$c_1 = \mathbf{s}^T\mathbf{u} + e' + M \cdot \lfloor q/2 \rfloor$
return $C = (\mathbf{c}_0^T, c_1)$

$\mathsf{Decrypt}(sk, C)$:

$m = c_1 - \mathbf{c}_0^T\mathbf{x}$
return $\begin{cases} 0 \text{ if } m \text{ is closer to 0 than to } \lfloor q/2 \rfloor \\ 1 \text{ otherwise} \end{cases}$

Correctness: To decrypt, we compute

$$m = c_1 - \mathbf{c}_0^T\mathbf{x} = \underbrace{e' - \mathbf{e}^T\mathbf{x}}_{small} + M \cdot \lfloor q/2 \rfloor.$$

The decryption holds if $\|e' - \mathbf{e}^T\mathbf{x}\|$ is less than $\lfloor q/4 \rfloor$.
Security: IND-CPA secure under the hardness of LWE.

A new signature scheme

$\mathsf{KeyGen}(1^\lambda)$:

$(\mathbf{A}, \mathbf{T}) \leftarrow \mathsf{TrapGen}(\mathbf{H} = \mathbf{0})$
return $vk = \mathbf{A}$ and $sk = \mathbf{T}$.

$\mathsf{Sign}(sk, M)$:

$\mathbf{A}_M = \mathbf{A} + (\mathbf{0} \,|\, H(M)\mathbf{G}) = \left(\mathbf{A}' \,|\, H(M)\mathbf{G} - \mathbf{A}'\mathbf{T}\right)$
$\mathbf{x} \leftarrow \mathsf{SamplePre}(\mathbf{R}, \mathbf{A}, \mathbf{H}, \zeta, \mathbf{0})$
return $\mathbf{x}$.

$\mathsf{Verify}(vk, \mathbf{x})$:

Accept iff $\mathbf{x} \neq \mathbf{0}$, $\mathbf{A}_M\mathbf{x} = \mathbf{0}$ and $\|\mathbf{x}\| \leq t\zeta\sqrt{m}$.

Correctness: With high probability, the norm of a signature is bounded by $t\zeta\sqrt{m}$ and hence is a valid signature.
Security: SU-CMA (Selective Unforgeability against Chosen Message Attack) secure under the hardness of ISIS.

A new IBE scheme [Ber+18]

IBE = Dual-Regev PKE + Signature

$\mathsf{Setup}(1^\lambda)$:

$(\mathbf{A}, \mathbf{T}) \leftarrow \mathsf{TrapGen}(\mathbf{H} = \mathbf{0})$
$\mathbf{u} \hookleftarrow U(\mathbb{Z}_q^n)$
return $mpk = (\mathbf{A}, \mathbf{u})$ and $msk = \mathbf{T}$.

$\mathsf{Extract}(msk, id)$:

$\mathbf{A}_{id} = \mathbf{A} + (\mathbf{0} \,|\, H(id)\mathbf{G})$
$= \left(\mathbf{A}' \,|\, H(id)\mathbf{G} - \mathbf{A}'\mathbf{T}\right)$
$\mathbf{x} \leftarrow \mathsf{SamplePre}(\mathbf{R}, \mathbf{A}, \mathbf{H}, \zeta, \mathbf{u})$
return $\mathbf{x}$.

$\mathsf{Encrypt}(mpk, id, M)$:

$C \leftarrow \mathsf{Encrypt}((\mathbf{A}_{id}, \mathbf{u}), M)$
return C

$\mathsf{Decrypt}(msk, sk_{id}, C)$:

$M \leftarrow \mathsf{Decrypt}(sk_{id}, C)$
return M

Timings in ms for the different operations of the IBE scheme (Setup, Extract Encrypt and Decrypt) and some precomputation operations (PreCompute).

(λ, n)	Setup	PreCompute	Extract	Encrypt	Decrypt
$(40, 512)$	0.93	1.32	2.27	0.45	0.0625
$(80, 1024)$	1.67	3.125	4.02	1.0	0.12
$(195, 2048)$	3.125	6.67	8.19	2.44	0.94

Experimental Result

Timings in ms for the different operations of the signature scheme (KeyGen, Sign and Verify) and some precomputation operations (PreCompute).

(λ, n)	KeyGen	PreCompute	Sign	Verify
$(60, 512)$	0.52	1.05	1.12	0.025
$(140, 1024)$	0.91	3.44	2.0	0.043
$(170, 1024)$	0.96	3.92	1.85	0.047

Instantiation

- use structure variant of the LWE/SIS problems,
- we use a computational argument (Learning with Errors problem) to hide the trapdoor matrix $\mathbf{T}$ into the public matrix $\mathbf{A}$
- we set the parameter t to ensure that the probability of falling in the tailcut is under $2^{-\lambda}$ where λ is the security parameter,
- we set all the parameters to ensure that the ISIS/LWE instances are hard.

Bibliography

[ABB10] Shweta Agrawal, Dan Boneh, and Xavier Boyen. "Efficient Lattice (H) IBE in the Standard Model". In: *EUROCRYPT* (2010).

[Ajt96] Miklós Ajtai. "Generating hard instances of lattice problems". In: *STOC* (1996).

[Ber+18] Pauline Bert et al. "Practical Implementation of Ring-SIS/LWE Based Signature and IBE". In: *PQCrypto* (2018).

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. "How to Use a Short Basis: Trapdoors for Hard Lattices and New Cryptographic Constructions". In: *STOC* (2008).

[MP12] Daniele Micciancio and Chris Peikert. "Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller". In: *EUROCRYPT* (2012).

[Reg05] Oded Regev. "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography". In: *STOC* (2005).