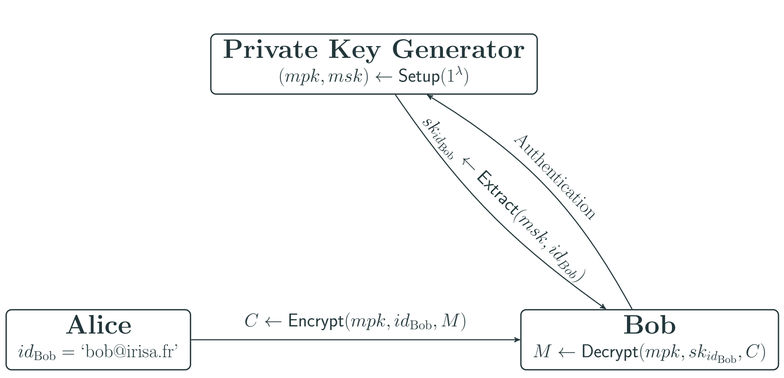
Identity Based Encryption from Lattices

Pauline Bert
Adeline Roux-Langlois & Pierre-Alain Fouque

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.

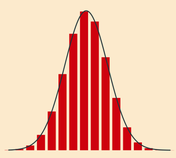
2017 First code based IBE, by Gaborit, Hauteville, Phan and Tillich

→ **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

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

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

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:

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

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

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

Trapdoor [Ajt96; MP12]

A public matrix $\mathbf{A}$ can be generated together with a **trapdoor** $\mathbf{T}$ thanks to the algorithm

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

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

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

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

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

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

- $\mathbf{G} \in \mathbb{Z}_q^{n\times nk}$ is a public **'gadget matrix'** associated to a structured basis,
- $\mathbf{H} \in \mathbb{Z}_q^{n\times n}$ is an **invertible tag**.

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 $pk = (\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x} \bmod q)$ 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 $\lfloor q/4 \rfloor$.

Semantic security:
According to the Leftover Hash Lemma, the public key $\mathbf{u} = \mathbf{A}\mathbf{x} \bmod q$ is statistically close to uniform and hides the secret key $\mathbf{x}$. The view $((\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x}), (\mathbf{c}_0^T = \mathbf{s}^T\mathbf{A} + \mathbf{e}^T, c_1 = \mathbf{s}^T\mathbf{u} + e' + M \cdot \lfloor q/2 \rfloor))$ of an adversary who wants to attack the scheme is simply $m + 1$ samples from the LWE distribution and hence computationally indistinguishable from uniform assuming 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 $sk = \mathbf{T}$.

$\mathsf{Sign}(sk, M)$:
$\mathbf{A}_M = \mathbf{A} + (\mathbf{0} \,|\, H(M)\mathbf{G})$
$= \left(\mathbf{A}' \,|\, H(M)\mathbf{G} - \mathbf{A}'\mathbf{T}\right)$
$\mathbf{x} \leftarrow \mathsf{SamplePre}(\mathbf{R}, \mathbf{A}, \mathbf{H}, \zeta, 0)$
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:
Thanks to the Gaussian tailcut, with high probability the norm of a signature outputted by SamplePre is bounded by $t\zeta\sqrt{m}$ and hence is a valid signature.

Security:
The security of this scheme is the **selective unforgeability against chosen message attack** (SU-CMA) based on the hardness of the ISIS problem. An adversary attacking the scheme choose a target message M^*, can issue signing queries on messages $M \neq M^*$ and has to create a valid forgery for the message M^*.

Instantiation

- the public matrix $\mathbf{A}$ has to hide the trapdoor matrix $\mathbf{T}$ by either a statistical (Leftover Hash Lemma) or a computational argument (Learning with Errors problem),
- the norm β of a secret key (or a signature) needs to ensure that the underlying ISIS instance is hard,
- the Gaussian parameter for the encryption needs to ensure that the underlying LWE instance is hard,
- the parameter t is chosen such that the probability of falling in the tailcut is under $2^{-\lambda}$ where λ is the security parameter, for e.g. for $t = 12$, the probability is under 2^{-100}.

A new IBE scheme

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

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: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (1996).

[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).