Public Key Encryption Schemes

Yanheng Wang

February 26, 2023

1 Assumptions

Definition. Let P, Q be two probability distributions over Ω, all parameterised by λ. Their *statistical distance* is defined as

$$\Delta(P, Q) := \sup_{A \subseteq \Omega} (P(A) - Q(A)).$$

We say P, Q are *statistically close* if $\Delta(P, Q)$ is a negligible function in λ.

One can paraphrase $\Delta(P, Q)$ in the lanaguage of games. Someone samples $a \sim P$ with half probability or $a \sim Q$ with the other half probability. Upon seeing a, we want to tell if the person went for the first option. Suppose our strategy is deterministic, and we answer "yes" when $a \in A$, and "no" when $a \notin A$. Then our answer is correct with probability

$$\frac{1}{2} P(A) + \frac{1}{2} Q(\Omega \setminus A) = \frac{1}{2} + \frac{P(A) - Q(A)}{2}.$$

So our "advantage" over a blind guess is captured by the difference $P(A) - Q(A)$. Hence $\Delta(P, Q)$ can be interpreted as the maximum advantage of all possible strategies.

In general, the "smartest" strategy A will not admit a concise description than enumerating all elements in A, which is of course not computationally realistic. If we restrict A to be efficiently computable, then we arrive at another closeness notion:

Definition. Let P, Q be two probability distributions over Ω, all parameterised by λ. We say they are *computationally close*, denoted $P \approx Q$, if for all $A \subseteq \Omega$ computable in $\mathrm{poly}(\lambda)$ time, the advantage $P(A) - Q(A)$ is a negligible function in λ.

Remark. One might wonder defining "computational distance" $\delta(P, Q) := \sup_A (P(A) - Q(A))$ where the supremum is over all efficiently computable A. But this definition does not make sense because λ is held constant in the supremum and thus the word "efficient" is meaningless.

Proposition. Statistical closeness implies computational closeness.

Proposition. The relation $\approx$ is transitive.

DDH Assumption. The following two distributions are computationally close:

- (g^a, g^r, g^{ar}) where $a, r \in \mathbb{Z}_p$ are uniform;
- (g^a, g^r, θ) where $a, r \in \mathbb{Z}_p$ and $\theta \in \mathbb{G}$ are uniform.

BDDH Assumption. The following two distributions are computationally close:

- $(g^a, g^r, h^a, h^b, \langle g, h \rangle^{abr})$ where $a, b, r \in \mathbb{Z}_p$ are uniform;

– $(g^a, g^r, h^a, h^b, \theta)$ where $a, b, r \in \mathbb{Z}_p$ and $\theta \in \mathbb{G}$ are uniform.

LWE Assumption. If $0 < {}^B/_q < 1$ is sufficiently large, then the following two distributions are computationally close:

– $(A, A\,s + e)$ where $A \in \mathbb{Z}_p^{m \times n}$, $s \in \mathbb{Z}_p^n$, $e \in [-B, B]^m$ are uniform;

– $(A, u) \in \mathbb{Z}_p^{m \times (n+1)}$ uniform.

Leftover Hash Lemma. Suppose $m \geqslant n \log q + 2\,\lambda$ and define

P. $(A, R\,A)$ where $A \in \mathbb{Z}_p^{m \times n}$, $R \in \{0,1\}^{t \times m}$ are uniform;

Q. (A, U) where $A \in \mathbb{Z}_p^{m \times n}$, $U \in \mathbb{Z}_p^{t \times n}$ are uniform.

Then $\Delta(P, Q) \leqslant t \cdot 2^{-\lambda}$, so the two distributions are statistically close.

Smudging Lemma. Fix any $x \in [-B, B]^n$. Define

P. $\varepsilon \in [-\hat{B}, \hat{B}]^n$ uniform;

Q. $x + \varepsilon$ for $\varepsilon \in [-\hat{B}, \hat{B}]^n$ uniform.

Then $\Delta(P, Q) \leqslant \frac{n\,B}{2\,\hat{B}}$. In particular, the two distributions are statistically close if we choose, say, $\hat{B} \geqslant n\,2^{\lambda} \cdot B$.

2 Constructions

2.1 Basic Schemes

***Scheme* ElGamal**		
secret key	a	$a \in \mathbb{Z}_p$ random
public key	g^a	
encryption	$c_1 := g^r$	$r \in \mathbb{Z}_p$ random
	$c_2 := g^{a\,r} \cdot \mu$	
decryption	c_2 / c_1^a	

Assume $m \geqslant N + 2\,\lambda$ and $B \leqslant \frac{p}{4\,m}$.

***Scheme* Regev**		
secret key	s	$A \in \mathbb{Z}_p^{m \times n}$, $s \in \mathbb{Z}_p^n$, $e \in [-B, B]^m$ random
public key	$A,\ A\,s + e$	
encryption	$c_1 := r^{\mathrm{T}} A$	$r \in \{0,1\}^m$ random
	$c_2 := r^{\mathrm{T}}(A\,s + e) + \frac{\mu\,p}{2}$	
decryption	$\mathbb{1}\left\{\lvert c_2 - c_1\,s\rvert \geqslant \frac{p}{4}\right\}$	

Further assume $\hat{B} := 2^{\lambda} \cdot B \leqslant \frac{p}{4\,m}$.

Scheme **Regev-dual**		
secret key	r	$A\in\mathbb{Z}_p^{m\times n}$, $r\in\{0,1\}^m$ random
public key	$A,\ r^{\mathrm{T}}A$	
encryption	$c_1 := A\,s+e$ $c_2 := r^{\mathrm{T}}A\,s+\varepsilon+\frac{\mu\,p}{2}$	$s\in\mathbb{Z}_p^n$, $e\in[-B,B]^m$, $\varepsilon\in[-\hat{B},\hat{B}]$ random
decryption	$\mathbb{1}\left\{\lvert c_2-r^{\mathrm{T}}c_1\rvert\geqslant\frac{p}{4}\right\}$	

2.2 Fully Homomorphic Encryptions (FHE)

Denote $N := (n+1)\log p$ and assume

- $m\geqslant N+2\,\lambda$;
- $B\leqslant\frac{p}{4\,m\,(N+3)^d}$ where d is the largest tolerated circuit depth.

Scheme **FHE**		
secret key	s	$A\in\mathbb{Z}_p^{m\times n}$, $s\in\mathbb{Z}_p^n$, $e\in[-B,B]^m$ random
public key	$A,\ A\,s+e$	
encryption	$C := R\,(A, A\,s+e)+\mu\,G$	$R\in\{0,1\}^{N\times m}$ random $G\in\mathbb{Z}_p^{N\times(n+1)}$ the gadget matrix
addition	$C+C'$	
multiplication	$\mathtt{bin}(C)\,C'$	$\mathtt{bin}(C)\in\{0,1\}^{N\times N}$ is the binary decomposition of C
decryption	$\mathbb{1}\left\{\left\lvert c^{\mathrm{T}}\begin{pmatrix} s\\ -1\end{pmatrix}\right\rvert\geqslant\frac{p}{4}\right\}$	$c^{\mathrm{T}}\in\mathbb{Z}_p^{1\times(n+1)}$ the last row of C

2.3 Identity-Based Encryptions (IBE)

Scheme **IBE-Boneh-Franklin**		
secret key	a	$a\in\mathbb{Z}_p$ random
public key	$g^a,\ \langle\cdot,\cdot\rangle,\ H$	$\langle\cdot,\cdot\rangle:\mathbb{G}\times\mathbb{H}\rightarrow\mathbb{T}$ pairing $H:\{0,1\}^*\rightarrow\mathbb{H}$ hash oracle
user key	$k := H(i)^a$	
encryption	$c_1 := g^r$ $c_2 := \langle g^{ar}, H(i)\rangle\cdot\mu$	$r\in\mathbb{Z}_p$ random
decryption	$c_2/\langle c_1,k\rangle$	

Scheme **IBE-pairing**		
secret key	a,b,u	$a,b,u\in\mathbb{Z}_p$ random
public key	$\langle\cdot,\cdot\rangle,\ \langle g^a,h^b\rangle,\ g^a,\ g^u$	$\langle\cdot,\cdot\rangle:\mathbb{G}\times\mathbb{H}\rightarrow\mathbb{T}$ pairing
user key	$k_0 := h^{ab+(u+ai)s}$ $k_1 := h^s$	$s\in\mathbb{Z}_p$ random
encryption	$c_0 := g^r$ $c_1 := g^{(u+ai)r}$ $\varsigma := \langle g^a,h^b\rangle^r\cdot\mu$	$r\in\mathbb{Z}_p$ random
decryption	$\varsigma\cdot\langle c_1,k_1\rangle/\langle c_0,k_0\rangle$	

Denote $N := n \log p$, $D := 2^{\lambda} N$, and assume

- $m \geqslant N + 2\lambda$;
- $B \leqslant \frac{p}{4mD}$.

***Scheme* IBE-Gentry-Peikert-Vaikuntanathan**		
secret key public key	R $A := \begin{pmatrix} U \\ RU + G \end{pmatrix}, H$	$R \in \{0,1\}^{N \times m}$, $U \in \mathbb{Z}_p^{m \times n}$ $G \in \mathbb{Z}_p^{N \times n}$ gadget matrix $H : \{0,1\}^* \to \mathbb{Z}_p^n$ hash oracle
user key	$k^{\mathrm{T}} := (-v^{\mathrm{T}} R, v^{\mathrm{T}}) + \delta^{\mathrm{T}}$	$\delta \in [-D, D]^m$ random $v^{\mathrm{T}} := \mathtt{bin}(H(i)^{\mathrm{T}} - \delta^{\mathrm{T}} A)$
encryption	$c_1 := A s + e$ $c_2 := H(i)^{\mathrm{T}} s + \frac{\mu p}{2}$	$s \in \mathbb{Z}_p^n$, $e \in [-B, B]^m$ random
decryption	$\mathbb{1}\{\lvert c_2 - k^{\mathrm{T}} c_1 \rvert \geqslant \frac{p}{4}\}$	

Note that the user key k^{T} of identity i satisfies

$$\begin{aligned} k^{\mathrm{T}} A &= -v^{\mathrm{T}} R U + v^{\mathrm{T}} R U + v^{\mathrm{T}} G + \delta^{\mathrm{T}} A \\ &= H(i)^{\mathrm{T}} - \delta^{\mathrm{T}} A + \delta^{\mathrm{T}} A \\ &= H(i)^{\mathrm{T}}. \end{aligned}$$

2.4 Hierarchical IBE (HIBE)

Assume the identity i is represented as a bit string $i_1 \ldots i_\ell$.

***Scheme* HIBE-pairing**		
secret key public key	$ab, u_1, \ldots, u_\ell$ $\langle \cdot, \cdot \rangle$, $\langle g^a, h^b \rangle$, g^a, $g^{u_1}, \ldots, g^{u_\ell}$, h^a	$a, b, u_1, \ldots, u_\ell \in \mathbb{Z}_p$ random $\langle \cdot, \cdot \rangle : \mathbb{G} \times \mathbb{H} \to \mathbb{T}$ pairing
user key	$k_0 := h^{ab + \sum_j (u_j + a i_j) s_j}$ $k_j := h^{s_j}$ for $j \in [\ell]$	$s_1, \ldots, s_\ell \in \mathbb{Z}_p$ random
encryption	$c_0 := g^r$ $c_j := g^{(u_j + a i_j) r}$ for $j \in [\ell]$ $\varsigma := \langle g^a, h^b \rangle^r \cdot \mu$	$r \in \mathbb{Z}_p$ random
decryption	$\varsigma \cdot \prod_j \langle c_j, k_j \rangle / \langle c_0, k_0 \rangle$	

2.5 Fuzzy IBE (FIBE)

Assume that any identity i is represented as a bit string $i_1 \ldots i_\ell$. Denote by $\mathrm{dist}(i, i')$ the Hamming distance between i and i'. The fuzzy IBE allows decryption whenever $\mathrm{dist}(i, i') < d$, where i is the identity at the time of encryption and i' is the identity of the user key.

***Scheme* FIBE (sketch)**
function `setup`()
sample matrices A_j^0, A_j^1 and preimage trapdoors R_j^0, R_j^1 for each index $j \in [\ell]$
sample $u \in \mathbb{Z}_p^n$
use $\{A_j^b\}, u$ as public key
use $\{R_j^b\}$ as secret key
function `split`(i)
generate fresh shares $u \rightsquigarrow u_1, \ldots, u_\ell$ with threshold $\ell - d$
find preimage $k_j : k_j^{\mathrm{T}} A_j^{i_j} = u_j$ by trapdoors, for all $j \in [\ell]$
return $\{k_j\}, i$ as the user key for identity i
function `encrypt`(μ, i)
sample $s, \{e_j\}, \varepsilon$
let $\varsigma := u^{\mathrm{T}} s + \varepsilon + \frac{\mu p}{2}$
return $\{A_j^{i_j} s + e_j\}, \varsigma, i$
function `decrypt`(c)
suppose $\{k_j\}, i'$ is the user key
let $J := \{j \in [\ell] : i_j = i'_j\}$
compute reconstruction coefficients $\{\alpha_j\}$ so that $\sum_{j \in J} \alpha_j u_j = u$
return 1 iff $\varsigma - \sum_{j \in J} \alpha_j \cdot k_j (A_j^{i_j} s + c_j) \geqslant \frac{p}{4}$

3 Transformations

3.1 IBE + signature ⇒ CC security

***Scheme* Canetti-Halevi-Katz**
function `setup`()
$(\mathrm{sk}, \mathrm{pk}) :=$ `IBE.setup`()
return $(\mathrm{sk}, \mathrm{pk})$
function `encrypt`($\mu \mid \mathrm{pk}$)
$(v, s) :=$ `SIG.setup`()   *{verification & signing keys}*
$c :=$ `IBE.encrypt`($\mu, v \mid \mathrm{pk}$)   *{use v as identity}*
$\sigma :=$ `SIG.sign`($c \mid s$)
return (c, σ, v)
function `decrypt`($c, \sigma, v \mid \mathrm{sk}$)
if not `SIG.verify`($c, \sigma \mid v$) **then**
return $\perp$
else
$k :=$ `IBE.split`($v \mid \mathrm{sk}$)
return `IBE.decrypt`($c \mid k$)

3.2 IBE + FHE ⇒ distributed IBE

***Scheme* Distributed-IBE**

function `setup`()
  $(\mathrm{sk}, \mathrm{pk}) := \mathtt{IBE.setup}()$
  $(\mathrm{sk}', \mathrm{pk}') := \mathtt{FHE.setup}()$
  sample $s_1, \ldots, s_n$ subject to $\sum_j s_j = \mathrm{sk}'$
  $e := \mathtt{FHE.enc}(\mathrm{sk} \mid \mathrm{sk}')$
  use (s_j, e) as secret key for party $j \in [n]$
  use $(\mathrm{pk}, \mathrm{pk}')$ as public key

function `split`$(i \mid s_j, e)$
  define function $f : x \mapsto \mathtt{IBE.split}(i \mid x)$
  $\tilde{e} := \mathtt{FHE.evaluate}(f, e \mid \mathrm{pk}')$ {*$\tilde{e}$ encrypts the user key of i*}
  $k_j := \mathtt{FHE.partial\text{-}decrypt}(\tilde{e} \mid s_j)$
  return k_j

function `encrypt`$(\mu, i \mid \mathrm{pk})$
  return $\mathtt{IBE.encrypt}(\mu, i \mid \mathrm{pk})$

function `decrypt`$(c \mid k_1, \ldots, k_n)$
  $k := \mathtt{FHE.assemble}(k_1, \ldots, k_n)$
  return $\mathtt{IBE.decrypt}(c \mid k)$

4 Security Notions

CM security Fix an efficient attacker, and consider two interations

referee		attacker
$(\mathrm{sk}, \mathrm{pk}) := \mathtt{setup}()$	$\rightarrow$	see pk
get $\mu^\star$	$\leftarrow$	compute $\mu^\star$
$c^\star := \mathtt{encrypt}(\mu^\star \mid \mathrm{pk})$	$\rightarrow$	see $c^\star$

referee		attacker
$(\mathrm{sk}, \mathrm{pk}) := \mathtt{setup}()$	$\rightarrow$	see pk
ignore; resample $\mu^\star$	$\leftarrow$	compute $\mu^\star$
$c^\star := \mathtt{encrypt}(\mu^\star \mid \mathrm{pk})$	$\rightarrow$	see $c^\star$

Let P (resp. Q) be the joint distribution of $(\mathrm{pk}, \mu^\star, c^\star)$ in the first (resp. the second) interaction. Both implicitly depend on the behaviour of the attacker. We say that the scheme resists this attacker if $P \approx Q$. It is *CM-secure* if it resists all efficient attackers.

All other security definitions follow the same pattern: Describe two interactions in which an attacker can participate, and require his views to be computionally close.

CC security

referee		attacker
$(\mathrm{sk}, \mathrm{pk}) := \mathtt{setup}()$	$\rightarrow$	see pk
return $\mathtt{decrypt}(c \mid \mathrm{sk})$	$\leftrightarrow$	enquire any c
get $\mu^\star$ / resample $\mu^\star$	$\leftarrow$	compute $\mu^\star$
$c^\star := \mathtt{encrypt}(\mu^\star \mid \mathrm{pk})$	$\rightarrow$	see $c^\star$
return $\mathtt{decrypt}(c \mid \mathrm{sk})$	$\leftrightarrow$	enquire any $c \neq c^\star$

Note that a homomorphic scheme cannot be CC-secure. We can design an attacker as follows. Given ciphertext $c^\star$ that contains message $\mu^\star$, he uses homomorphism to get a ciphertext c that contains message $\mu^\star + 1$, say. Then he ask the referee to decrypt c.

His two views are not computationally close, as the decryption contains essentially all information to distinguish the two.

IBE-CM security

referee		attacker
$(\mathrm{sk}, \mathrm{pk}) := \mathtt{setup}()$	$\rightarrow$	see pk
return $\mathtt{split}(i \mid \mathrm{sk})$	$\leftrightarrow$	enquire any identity i
get $i^\star$	$\leftarrow$	compute $i^\star$ not yet enquired
get $\mu^\star$ / resample $\mu^\star$	$\leftarrow$	compute $\mu^\star$
$c^\star := \mathtt{encrypt}(\mu^\star, i^\star \mid \mathrm{pk})$	$\rightarrow$	see $c^\star$
return $\mathtt{split}(i \mid \mathrm{sk})$	$\leftrightarrow$	enquire any identity $i \neq i^\star$