GPV signatures and IBE in the standard model

CR15

2019-2020

Contents

1 GPV Signatures

1.1 IBE implies signatures

Let an IBE (Setup, KeyGen, Encrypt, Decrypt).
We build a signature as follows:

- KeyGen(1^λ) :

  Run $(mpk, msk) \leftarrow \text{Setup}(1^\lambda)$
  Output : $pk = mpk,\ sk = msk$

- Sign(sk, M) :

  Run $sk_M \leftarrow \text{KeyGen}(msk, M)$
  Output : $sig = sk_M$

- Verify(pk, M, sig) :

  1. Choose a random message r
  Compute $c \leftarrow \text{Encrypt}(mpk, M, r)$
  2. Given $sig = sk_M$
  Compute $r' = \text{Decrypt}(mpk, sk_M, c)$
  If $r' = r$, return 1
  If $r' \neq r$, return 0

Theorem 1. *If the IBE is IND-ID-CPA, the signature is secure under chosen-message attacks.*

Remark. *In most cases, Verify can be written deterministically.*

1.2 GPV Signatures

- KeyGen(1^n) :

  1. Choose a modulus $q \geq 3$ prime and m $\geq 6nlog(q)$
  Choose a standard deviation $\sigma > \omega(\sqrt{log(m)})$
  2. Run $(A, T_A) \leftarrow \text{TrapGen}(1^n, 1^m, \sigma)$ to get $A \sim U(\mathbb{Z}_q^{n \times m})$
  and $T_A \in \mathbb{Z}^{m \times m}$ a short basis of $\Lambda_q^{\perp}(A)$ such that $\|\tilde{T}_A\| \leq O(\sqrt{nlog(q)})$
  Output $pk = (A, h)$ and $sk = T_A$ where $h : \{0,1\}^* \rightarrow \mathbb{Z}_q^n$

- Sign(sk, M) :

  1. Compute $u_M = h(M) \in \mathbb{Z}_q^n$
  2. Run a deterministic variant of $v \leftarrow \text{SamplePre}(A, T_A, u_M, \sigma)$
  to get $v \in \Lambda_q^{u_M}(A)$ with a distribution statistically close to $D_{\Lambda_q^{u_M}(A), \sigma}$
  Output $sig = v \in \mathbb{Z}^m$

- Verify(pk, M, sig) :

$$\text{return 1 iff} \begin{cases} 1)\ A.v = h(M) \in \mathbb{Z}_q^n \\ 2)\ \|v\| \leq \sigma\sqrt{m} \text{ and } v \neq 0^m \end{cases}$$

Remark. *Sign must be derandomized since only one signature should be revealed for any M. Otherwise, revealing $v, v' \in \mathbb{Z}^m$ such that $A.v = A.v'(mod\ q)$ would leak $v - v' \in \Lambda_q^{\perp}(A)$.*

Theorem 2. *The scheme is secure under chosen-message attacks in the random oracle model under the $SIS_{q,n,m,\beta}$ with $\beta = \tilde{O}(n)$.*

Lemma 1. *(Peikert-Rosen,2006): Let q prime and $m > 6nlog(q)$. Let $A \sim U(\mathbb{Z}_q^{n\times m})$ and $\sigma > \omega(\sqrt{log(m)})$, for any $u \in \mathbb{Z}_q^n$ and $y \in \mathbb{Z}^m$,*

$$\Pr_{x\sim D_{\Lambda_q^u(A),\sigma}}[x = y] \leq 2^{-\Omega(n)}$$

Proof. (of Theorem 2)

Let $\mathscr{A}$ an adversary with advantage ϵ, we build a SIS solver B with advantage $\epsilon - 2^{-\Omega(n)}$.
B inputs $A \in \mathbb{Z}_q^{n\times m}$ and has to find $v \neq 0^m$ of norm $\|v\| < B$ such that $A.v = 0(mod\ q)$.
B defines $pk = A \in Z_q^{n\times m}$ and simulates $\mathscr{A}$'s new as follows:

- Hash queries: At each query H(M), B samples $e_M \leftarrow D_{\mathbb{Z}^m,\sigma}$ and returns $H(M) = u_M = A.e_M\ mod\ q$ and stores (M, u_M, e_M) in list L.
- Signing queries: At each signing query, we assume with high probability that $h(m)$ was queried before. Then, B retrieves (M, u_M, e_M) in list L and returns $e_M \in \mathbb{Z}^m$ (note that $A.e_M = u_M \pmod q$).
  We have $\|e_M\| \leq \sigma(\sqrt{m})$ since $e_M \sim D_{\Lambda_q^{u_M}(A),\sigma}$ (up to negligible statistical distance).
- Forgery: $\mathscr{A}$ outputs $(M^*, sig = e^*)$ with probability ϵ. We assume with high probability that $h(M^*)$ was queried. Then, L contains $(M^*, u_{M^*} \in \mathbb{Z}_q^n, e_{M^*} \in \mathbb{Z}_q^m)$.

Note that $\mathscr{A}$ obtained no signatures on M^*.

Conditionally on $u_{M^*} = h(M^*) \in \mathbb{Z}_q^n$, the distribution of $e_{M^*} \in \mathbb{Z}^m$ is $D_{\Lambda_q^{u_{M^*}}(A),\sigma}$ in $\Lambda_q^{u_{M^*}}(A)$. By the Peikert-Rosen Lemma, $Pr[e_{M^*} = e^*] \leq 2^{-\Omega(n)}$. Since $e = e^*$ with probability $1 - 2^{-\Omega(n)}$, we have $A.(\underbrace{e_{M^*} - e^*}_{\neq 0}) = 0 \pmod q$ and $\|e_{M^*} - e^*\| \leq 2\sigma\sqrt{m}$.
$\implies v^* = e_{M^*} - e^* \in \mathbb{Z}^m$ is a valid SIS solution with probability $\epsilon - 2^{-\Omega(n)}$. □

Remark. *Security proof is tight: no loss $\theta(Q_H)$ in the reduction as in the GPV-IBE.*

2 IBE in the standard model from LWE

2.1 Basis delegation algorithm

Given a short basis of $\Lambda_q^\perp(A)$, one can compute a short basis of $\Lambda_q^\perp([A|B])$.

Theorem 3. *(Cash-Hofheinz-Kiltz-Peikert, 2010): Let integers n,m,q such that $q \geq 3$ (prime) and $m \geq n$. Let $A \in \mathbb{Z}_q^{n\times m}$ with rank n. There is a PPT algorithm ExtBasis that inputs $T_A \in \mathbb{Z}^{n\times m}$ of $\Lambda_q^\perp(A)$ and a matrix $B \in \mathbb{Z}_q^{n\times k}$. It outputs a basis $T_{\overline{A}} \in \mathbb{Z}^{(m+k)\times(m+k)}$ of $\Lambda_q^\perp(\overline{A})$ where $\overline{A} = [A|B] \in \mathbb{Z}_q^{n\times(m+k)}$, such that $\|\tilde{T}_{\overline{A}}\| = \|\tilde{T}_A\|$*

Remark. *In particular, a short basis $T_A \in \mathbb{Z}^{m\times m}$ of $\Lambda_q^\perp(A)$ allows sampling from $D_{\Lambda_q^\perp([A|B]),\sigma}$*

Idea.

- *Sample many $b_i \leftarrow D_{\mathbb{Z}^k,\sigma}$ to compute $B.b_i \in \mathbb{Z}_q^m$ and use T_A to sample $v_i \in \mathbb{Z}^m$ Gaussian such that $A.v_i = -B.b_i \ (mod\ q)$.*
  $\implies \begin{bmatrix} v_i \\ b_i \end{bmatrix} \in \mathbb{Z}^{m+k}$ *satisfy* $[A|B].\begin{bmatrix} v_i \\ b_i \end{bmatrix} = 0$.
- *Given a set of $m+k$ independent $\begin{bmatrix} v_i \\ b_i \end{bmatrix} \in \Lambda_q^\perp([A|B])$, we can obtain a basis.*
- *Basis of $\Lambda_q^\perp([A|B])$ should be randomized to be independent of T_A*

Lemma 2. *(Agrawal-Boneh-Boyen,2010): Let n, m, k, q such that $k > n$, $m > 2n\log q$ and $q \geq 3$ prime. For any $A \in \mathbb{Z}_q^{n\times m}$ and $R \in \{-1,1\}^{n\times k}$, there is a PPT algorithm that inputs a full-rank $B \in \mathbb{Z}_q^{n\times k}$ and a basis $T_B \in \mathbb{Z}^{k\times k}$ of $\Lambda_q^\perp(B)$ such that $\|\tilde{T}_B\| \leq O(\sqrt{n\log(q)})$. For any $\sigma > \|\tilde{T}_B\|.\omega(\sqrt{n\log(m)})$, it samples $e \sim D_{\Lambda_q^\perp(\overline{A}),\sigma}$ in $\Lambda_q^\perp(\overline{A})$ where $\overline{A} = [A|A.R+B] \in \mathbb{Z}_q^{n\times(m+k)}$*

Remark. *For any $u \in \mathbb{Z}_q^m$, T_B allows sampling a short $e \in \mathbb{Z}^{m+k}$ such that*

$$\underbrace{[A|A.R+B]}_{\overline{A}}.e = u \pmod q$$

using $R \in \{-1,1\}^{n\times k}$

2.2 Gadget Matrix

(Micciancio-Peikert, 2012) Let a modulus q and $k = \lceil \log\ q \rceil$

Define $g^T = [1, 2, ..., 2^{k-1}] \in \mathbb{Z}_q^{1\times k}$ and $G = I_n \bigotimes g^T = \begin{pmatrix} g^T & & 0 \\ & \ddots & \\ 0 & & g^T \end{pmatrix} \in \mathbb{Z}^{n\times mk}$

Then $\Lambda_q^\perp(G)$ has a public short basis. Let $S_k = \begin{pmatrix} 2 & & & q_0 \\ -1 & 2 & & q_1 \\ & \ddots & \ddots & \vdots \\ & & -1 & q_{k-1} \end{pmatrix}$

where $(q_0, \ldots, q_{k-1}) \in \{0,1\}^k$ is the bit representation of $q = \Sigma_{i=0}^{k-1} q_i 2^i$.

We have $\begin{cases} g^T.S_k = 0\ mod\ q \\ \|s_i\| = \sqrt{5}\ for\ i < k\ and\ \|s_k\| < \sqrt{k} \end{cases}$

$\implies T_G = I_n \bigotimes S_k$ is short basis of $\Lambda_q^\perp(G)$

2.3 Full-rank difference matrix

Let q a prime, and an integer m, there is a function $H : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n\times n}$ such that for any $u, v \in \mathbb{Z}_q^n$ such that $u \neq v$, we have $H(u) - H(v) \in \mathbb{Z}_q^{n\times n}$ full rank over $\mathbb{Z}_q$.
Outline : Given $u^T = (u_0, u_1, \ldots, u_{n-1}) \in \mathbb{Z}_q^n$, define $u(X) = \Sigma_{i=0}^{n-1} u_i X^i \in \mathbb{Z}_q[X]$
Let $f \in \mathbb{Z}_q[X]$ irreducible of degree n in $\mathbb{Z}_q[X]$

$$H(u) = \begin{pmatrix} \text{coeffs}(U(X)) \\ \text{coeffs}(X.U(X)\ mod\ f) \\ \vdots \\ \text{coeffs}(X^{n-1}.U(X)\ mod\ f) \end{pmatrix} \in \mathbb{Z}_q^{n\times n}$$

2.4 Selectively-secure IBE

In the standard model (Agrowel-Boneh-Boyen, 2010)

- Setup(1^n)

  1. Choose $q \geq 3$ prime, a dimension $m \geq 2n \log\ q$, a standard deviation $\sigma > 0$, a parameter $\alpha \in (0, 1)$
  2. Run$(A_0, T_0) \leftarrow$ TrapGen$(1^n, 1^m, \sigma)$ to get $A_0 \sim U(\mathbb{Z}_q^{n\times m})$ with $T_{A_0} \in \mathbb{Z}^{m\times m}$ a basis of $\Lambda_q^{\perp}(A_0)$ such that $\|\tilde{T}_{A_0}\| < O(\sqrt{n \log\ q})$
  3. Choose $A_1 \leftarrow U(\mathbb{Z}_q^{n\times nk})$ with $k = \lceil \log\ q \rceil$
  $u \leftarrow U(\mathbb{Z}_q^n)$ and let $G = I_n \bigotimes [1, 2, 4, \ldots, 2^{k-1}]$
  4. Let $H : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n\times n}$ a full-rank difference function
  Output $mpk = (q, n, m, \sigma, \alpha, A_0, A_1, u),\ msk = T_{A_0}$.

- KeyGen(msk, ID)

  1. Given $ID \in \mathbb{Z}_q^n$, let $A_{id} = [A_0 | A_1 + H(ID).G] \in \mathbb{Z}_q^{n\times(m+nk)}$ where $H(ID) \in \mathbb{Z}_q^{n\times n}$
  2. Using $msk = T_{A_0}$, sample $e_{ID} \sim D_{\Lambda_q^u(A_i d),\sigma}$ to get $e_{ID} \in \mathbb{Z}^{m+nk}$ Gaussian such that $A_{id}.e_{ID} = u \bmod q$
  Return $sk_{ID} = e_{ID}$.

- Encrypt(mpk, ID, u) To encrypt $\mu \in \{0,1\}$

  1. Define $A_{id} = [A_0 | A_1 + H(ID).G] \in \mathbb{Z}_q^{n \times (m+nk)}$
  2. Choose $s \leftarrow U(\mathbb{Z}_q^n), R \leftarrow U(\{-1,1\}^{m \times nk})$

     $x \leftarrow \chi$

     $y \leftarrow \chi^m$

     Define $z = R^T y \in \mathbb{Z}^{nk}$
  3. Compute $C_0 = u^T s + x + \mu \lfloor \frac{q}{2} \rfloor \in \mathbb{Z}_q$

  $$C_1 = A_{id}^T \cdot s + \begin{pmatrix} y \\ z \end{pmatrix} \in \mathbb{Z}_q^{n+nk}$$

  $$= \begin{pmatrix} A_0^T \\ A_1^T + G^T H(ID)^T \end{pmatrix} s + \begin{pmatrix} y \\ R^T y \end{pmatrix}$$

  Output $(C_0, C_1) \in \mathbb{Z}_q \times \mathbb{Z}_q^{m+nk}$.

- Decrypt(mpk, sk_{ID}, c)

  Given $sk_{ID} = e_{ID} \in \mathbb{Z}^{m+nk}$ short such that $[A_0 | A_1 + H(ID)G] \cdot e_{ID} = u \bmod q$,

  1. Compute $\mu' = C_0 - e_{ID}^T . C_1 \bmod q$
  2. If $|\mu' - \lfloor \frac{q}{2} \rfloor| < \frac{q}{4}$, output 1.

  Otherwise, output 0.

Correctness: Same as in GPV.