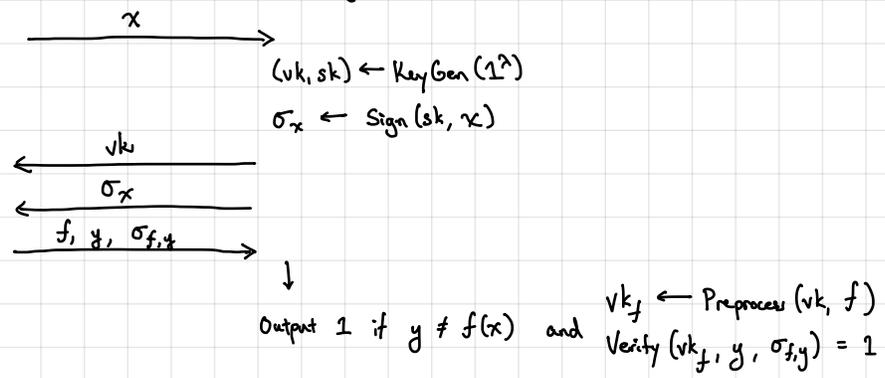


Decouple into two equations:

- Input-independent evaluation: $B_1, \dots, B_\ell, f \mapsto B_f$
 - Input-dependent evaluation: $[B_1 - x_1 G \mid \dots \mid B_\ell - x_\ell G] H_{f,x} = B_f - f(x) \cdot G$
-] Will give us many advanced primitives!

Unforgeability: Will consider a weaker (selective) notion of security where the message that is signed is independent of the verification key
 [not difficult to get full adaptive security, but somewhat tedious]



Proof of unforgeability.
 (from LWE)

Can also give a proof from SIS.
 [HW Exercise]

- Hyb₀: real signature unforgeability game
- Hyb₁: instead of sampling B_1, \dots, B_ℓ uniformly, sample $R_1, \dots, R_\ell \leftarrow \{0,1\}^{m \times t}$ and set $B_i \leftarrow AR_i + x_i G$ it sets $vk = (A, B_1, \dots, B_\ell)$ and $\sigma = (R_1, \dots, R_\ell)$
- Hyb₂: instead of sampling (A, T) using TrapGen, challenger samples $\bar{A} \xleftarrow{R} \mathbb{Z}_q^{(m) \times m}$, $s \xleftarrow{R} \mathbb{Z}_q^{n-1}$, $e \leftarrow \chi^m \rightsquigarrow A \leftarrow \begin{bmatrix} \bar{A} \\ s^T \bar{A} + e \end{bmatrix}$ (LWE matrix)

Selective security: message is programmed into the vk

Hyb₀ $\stackrel{\approx}{\sim}$ Hyb₁ by LHL
 Hyb₁ $\stackrel{\approx}{\sim}$ Hyb₂ under LWE

Suppose A succeeds in Hyb₂. Namely A outputs R_i^*, f, y such that

$$AR^* = B_f - y \cdot G$$

where $y \neq f(x)$ and R^* is short. Let

$$R_{f,x} = [R_1 \mid \dots \mid R_\ell] H_{f,x}$$

Then, by construction,

$$AR_{f,x} = [B_1 - x_1 G \mid \dots \mid B_\ell - x_\ell G] H_{f,x} = B_f - f(x) \cdot G$$

Then, $AR^* - AR_{f,x} = (-1)^c \cdot G$ where $c \in \{0,1\}$ and $\underbrace{[-s^T \mid 1]} (AR^* - AR_{f,x}) = [-s^T \mid 1] \cdot G$

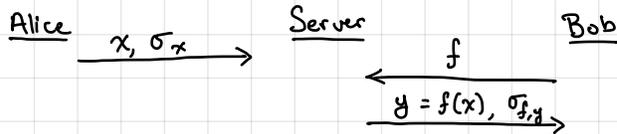
$$\underbrace{e^T (R^* - R_{f,x})}_{\substack{\text{small relative to } G \\ \text{since } e, R^*, R_{f,x} \text{ small}}} = [-s^T \mid 1] \cdot G \uparrow \substack{\text{has large} \\ \text{entries } (\frac{q}{2})}$$

Implication: in Hyb₂, scheme is statistically unforgeable!

Proof technique: programmed x into the public parameters
statistically unforgeable at $f(x)$ for all f
 \rightarrow could be forgeable on other messages: "somewhere unforgeable"

Context-hiding for homomorphic signatures:

- In many settings, we also want the computed signature to hide information about the input to the computation



Bob wants to check signature on $y = f(x)$ but should not learn anything about x

- We will see one application of this type of property to (designated-prover) NIZKs

We say a homomorphic signature scheme is ^{statistically} context-hiding if there exists an efficient simulator S where for all $(vk, sk) \leftarrow \text{KeyGen}(1^\lambda)$, $x \in \{0,1\}^l$, and $f: \{0,1\}^l \rightarrow \{0,1\}$:

$$\{vk, \text{Eval}(vk, f, \sigma)\} \stackrel{\approx}{\sim} \{vk, S(sk, vk, f, f(x))\}$$

↳ simulator needs to simulate valid signatures so it needs to know the signing key; however, it does not know the input x , only the value $f(x)$

Turns out this is not difficult to achieve!

↳ this means signature reveals no information about x other than $(f, f(x))$.

Current construction is not context-hiding:

$$R_{f,x} := [R_1 | \dots | R_\ell] \cdot H_{f,x}$$

↳ this is a function of x !

To achieve context-hiding, we need a way to re-randomize a signature.

Suppose $AR_{f,x} = B_f - y \cdot G$ where $y \in \{0,1\}$

Evaluator knows y so it can compute the matrix

$$V := [A | B_f + (y-1) \cdot G] = [A | AR_{f,x} + (2y-1) \cdot G]$$

Now, since $y \in \{0,1\}$, $2y-1 \in \{-1,1\}$. Then $R_{f,x}$ is a trapdoor for V :

$$V \cdot \begin{bmatrix} -R_{f,x} \\ \mathbf{I} \end{bmatrix} = (2y-1) \cdot G = G \text{ or } -G$$

The public key then includes a random target $z \xleftarrow{R} \mathbb{Z}_q^n$ and the signature is formed by sampling a short vector t such that $Vt = z$:

$$t \leftarrow \text{SamplePre}(V, \pm R_{f,x}, z, s) \text{ for some } s = (n \log q)^{O(d)}$$

To verify a signature, the verifier computes B_f from B_1, \dots, B_ℓ , constructs V from the verification key and checks that

$$Vt = z \text{ and } \|t\|_\infty \leq \beta \text{ where } \beta = (n \log q)^{O(d)} \text{ is the noise bound}$$

For context-hiding, we observe that $t \sim D_{\mathbb{Z}_q^{\pm}(H), s}$ where H only depends on $A, B_1, \dots, B_\ell, f, y$ (independent of x)

↳ We can sample from $D_{\mathbb{Z}_q^{\pm}(H), s}$ using a trapdoor for A (since V is an extension of A - see HW1)

Unforgeability: Follows by similar argument as before.

We argue selective security from LWE as before (can also argue security from SIS — see HW1)

Hyb₀: real unforgeability game

Hyb₁: after adversary chooses $x \in \{0,1\}^L$,

sample verification key as $[B_1 | \dots | B_L] = A[R_1 + x_1 G | \dots | R_L + x_L \cdot G]$

output $vk = (A, B_1, \dots, B_L, z)$ where $A \xleftarrow{R} \mathbb{Z}_q^{n \times m}$, $z \xleftarrow{R} \mathbb{Z}_q^n$

Hyb₂: sample A as an LWE matrix

$$A \leftarrow \begin{bmatrix} \bar{A} \\ \bar{s}^T \bar{A} + e^T \end{bmatrix} \quad \text{where } \bar{A} \xleftarrow{R} \mathbb{Z}_q^{(n-1) \times m} \quad e \xleftarrow{R} \mathbb{Z}_q^m \\ \bar{s} \xleftarrow{R} \mathbb{Z}_q^{n-1}$$

We show in Hyb₂ that advantage of any adversary A is negligible:

Suppose A outputs signature $\sigma = t$ on (f, y) where $y \neq f(x)$. [$f(x) = 1 - y$]

Let $V = [A | B_f + (y-1) \cdot G]$. Then $Vt = z$ (since signature verifies).

Let $R_{f,x} = [R_1 | \dots | R_L] \cdot H_{f,x}$. Then

$$\begin{aligned} AR_{f,x} &= A[R_1 | \dots | R_L] \cdot H_{f,x} = [B_1 - x_1 G | \dots | B_L - x_L G] H_{f,x} \\ &= B_f - f(x) \cdot G \\ &= B_f - (1-y) \cdot G \end{aligned}$$

$$\Rightarrow B_f = AR_{f,x} + (1-y) \cdot G$$

Then $V = [A | B_f + (y-1) \cdot G] = [A | AR_{f,x}]$ so $Vt = [A | AR_{f,x}]t$.

If $Vt = z$, then

$$s^T [A | AR_{f,x}]t = \boxed{s^T z} \quad (s = [-\bar{s} \ 1])$$

$$\underbrace{\begin{bmatrix} e^T & | & e^T R_{f,x} \end{bmatrix} t}_{\text{small (norm bounded by } (n \log q)^{O(d)})} \quad \leftarrow \text{large so long as } q \gg (n \log q)^{O(d)}$$

Recap: homomorphic encryption

$$pk: A = \begin{bmatrix} \bar{A} \\ \bar{s}^T \bar{A} + e^T \end{bmatrix}$$

$$ct: C = AR + \mu \cdot G$$

↑ ciphertext ↑ encryption ↑ message
↑ randomness

homomorphic signatures

$$vk: A \xleftarrow{R} \mathbb{Z}_q^{n \times m}$$

$$\text{signature: } AR = B - \mu \cdot G$$

↑ signature ↑ message

target matrix (in vk)

GSW homomorphisms are homomorphic on both messages and on randomness

$$C_1, \dots, C_L, f \mapsto C_f$$

$$[C_1 - x_1 G | \dots | C_L - x_L G] \cdot H_{f,x} = C_f - f(x) \cdot G$$

$$\parallel$$

$$A[R_1 | \dots | R_L] H_{f,x} \rightsquigarrow [R_1 | \dots | R_L] H_{f,x} = R_{f,x}$$

$$C_f = AR_{f,x} + f(x) \cdot G$$

homomorphism on message

homomorphism on randomness

HE: ciphertext evaluation

HS: verification

HS: signature evaluation