Let $\mathsf{UOV}_q(n,m)$ and $\mathsf{homogenousUOV}_q(n,m)$ be what their name suggests (as signature schemes, via an FDH-type construction, with no salting for simplicity). If it is necessary to define them wrt a security parameter λ, we leave q a prime power and $\rho > 2.5$ as free parameters, and set $(n,m) = (\lceil \rho\lambda \rceil, \lambda)$. Note that this implies that n, m, and also $n-m$ are $\Theta(\lambda)$.

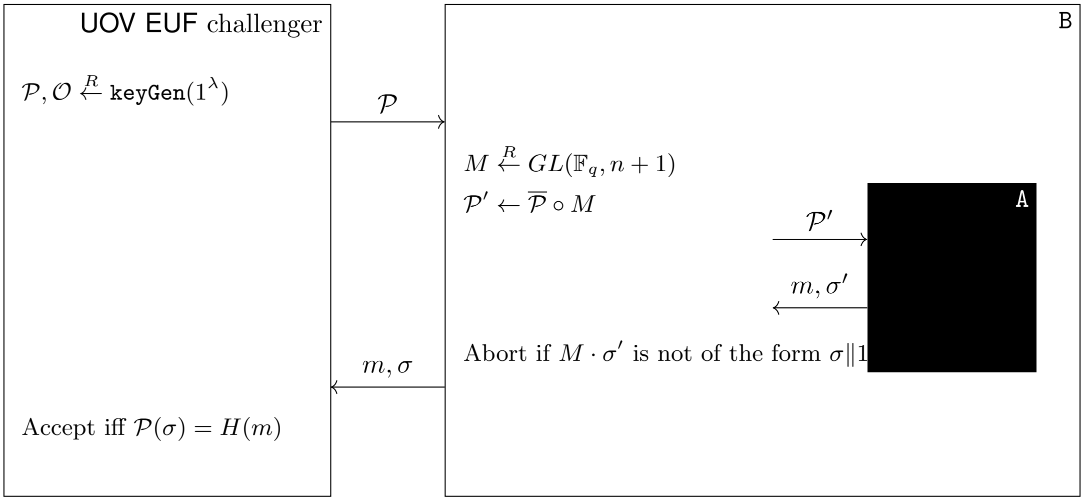
The idea is to show that $\mathsf{homogenousUOV}$ is at least as secure as UOV. We accomplish this through a direct reduction, but it's worthwhile to note that, even before this, there is good reason to assume that this is true. Indeed,

- All SOTA attacks against UOV are key-recovery attacks. These adapt without any loss in advantage from the inhomogenous to the homogenous setting.
- If one believes the usual assumptions for the security of UOV (namely: MQ is hard-on-average + instances of UOV are indistinguishable from instances of MQ), these imply analogous assumptions for the homogenous case (homogenousMQ is hard-on-average + instances of homogenousUOV are indistinguishable from instances of homogenousMQ).

Nonetheless, there is no direct reduction from UOV to homogenousUOV. Here we provide one (though it does need an extra security assumption, but it is a new and fairly natural security assumption). We will do reductions for EUF-KOA and EUF-CMA, though we claim these adapt seamlessly to the UUF and SUF settings (no claim about sEUF).

EUF-KOA

This one is straightforward:



UOV EUF challenger
$\mathcal{P}, \mathcal{O} \overset{R}{\leftarrow} \texttt{keyGen}(1^\lambda)$
$\mathcal{P}$
B
$M \overset{R}{\leftarrow} GL(\mathbb{F}_q, n+1)$
$\mathcal{P}' \leftarrow \overline{\mathcal{P}} \circ M$
A
$\mathcal{P}'$
m, σ'
Abort if $M \cdot \sigma'$ is not of the form $\sigma \| 1$
m, σ
Accept iff $\mathcal{P}(\sigma) = H(m)$

Figure 1

All that's necessary for the reduction to work is a couple observations about the distribution of $\mathcal{P}'$:

1. It is identical to the distribution of $\mathsf{homogenousUOV}$ public keys.
2. It is independent from the distribution of M.

(1) ensures that A produces a valid forgery with non-negligible probability, and (2) ensures that there's a 1/q chance that B can turn this into a forgery that remains valid in the inhomogenous setting (i.e. has the last coordinate set to 1).

EUF-CMA

We assume the hardness of $\mathsf{MH}_q(n)$ (q free, $n = \lambda$), the problem of distinguishing distributions from these two algorithms:

$$\mathtt{X}^1_q(n) : \mathtt{repeat}(x \overset{R}{\leftarrow} \mathbb{F}_q^n;\ \mathtt{yield}\ x)$$
$$\mathtt{X}^2_q(n) : V \overset{R}{\leftarrow} Gr(n-1, \mathbb{F}_q^n);\ \mathtt{repeat}(x \overset{R}{\leftarrow} \mathbb{F}_q^n \smallsetminus V;\ \mathtt{yield}\ x)$$

To use this, we start with the game of the adversary $\mathtt{A}$ playing against the challenger for the EUF-CMA security of homogenousUOV:

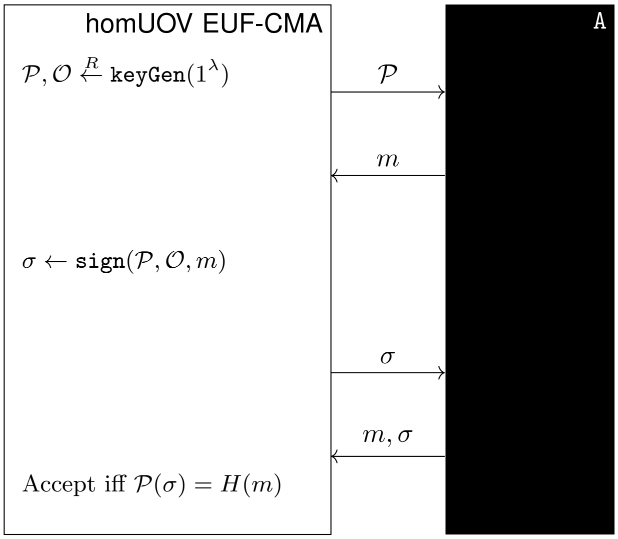
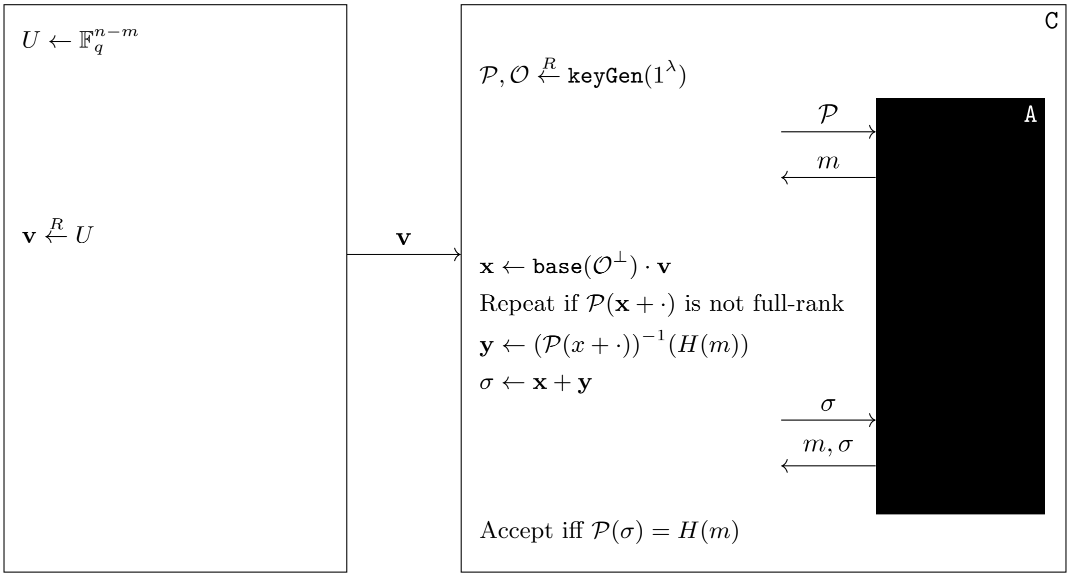

homUOV EUF-CMA
$\mathcal{P}, \mathcal{O} \overset{R}{\leftarrow} \mathtt{keyGen}(1^\lambda)$
$\mathcal{P}$
m
$\sigma \leftarrow \mathtt{sign}(\mathcal{P}, \mathcal{O}, m)$
σ
m, σ
Accept iff $\mathcal{P}(\sigma) = H(m)$
A

Figure 2

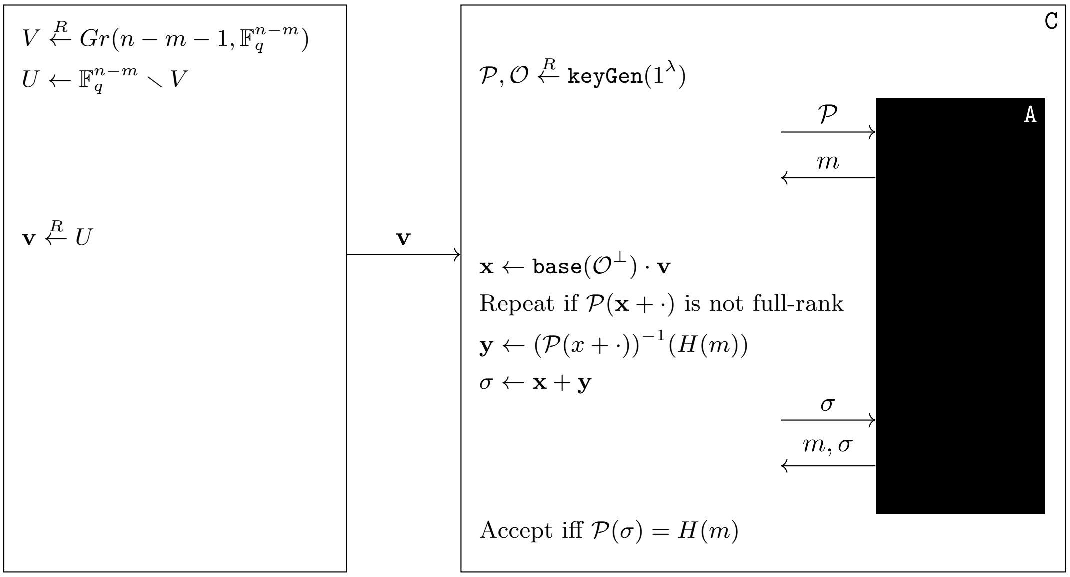
By assumption, there is a non-negligible probability that this accepts. We expand out the `sign` process and modify it until we arrive here:



$U \leftarrow \mathbb{F}_q^{n-m}$
$\mathbf{v} \overset{R}{\leftarrow} U$
$\mathbf{v}$
C
$\mathcal{P}, \mathcal{O} \overset{R}{\leftarrow} \texttt{keyGen}(1^\lambda)$
$\mathcal{P}$
A
m
$\mathbf{x} \leftarrow \texttt{base}(\mathcal{O}^\perp) \cdot \mathbf{v}$
Repeat if $\mathcal{P}(\mathbf{x} + \cdot)$ is not full-rank
$\mathbf{y} \leftarrow (\mathcal{P}(x + \cdot))^{-1}(H(m))$
$\sigma \leftarrow \mathbf{x} + \mathbf{y}$
σ
m, σ
Accept iff $\mathcal{P}(\sigma) = H(m)$

Figure 3

`base` is an algorithm (more of a notational artifact) that, given a subspace, returns a base of that subspace, as column vectors in a matrix. In any case, note that in the diagram above we have an adversary that samples from $\mathtt{X}_q^1(n-m)$, and either accepts or rejects. We can switch this out for $\mathtt{X}_q^2(n-m)$, and if MH_q is indeed hard, this should only negligibly change the adversary's probability of accepting, and thus the following game also accepts with non-negligible probability:



$V \overset{R}{\leftarrow} Gr(n-m-1, \mathbb{F}_q^{n-m})$
$U \leftarrow \mathbb{F}_q^{n-m} \setminus V$
$\mathbf{v} \overset{R}{\leftarrow} U$
$\mathbf{v}$
C
$\mathcal{P}, \mathcal{O} \overset{R}{\leftarrow} \texttt{keyGen}(1^\lambda)$
$\mathcal{P}$
A
m
$\mathbf{x} \leftarrow \texttt{base}(\mathcal{O}^\perp) \cdot \mathbf{v}$
Repeat if $\mathcal{P}(\mathbf{x} + \cdot)$ is not full-rank
$\mathbf{y} \leftarrow (\mathcal{P}(x + \cdot))^{-1}(H(m))$
$\sigma \leftarrow \mathbf{x} + \mathbf{y}$
σ
m, σ
Accept iff $\mathcal{P}(\sigma) = H(m)$

Figure 4

Another way of saying this is that, with the distribution of messages recieved by `A` in this game, there is a non-negligible probability that it outputs a valid forgery. Focusing, then, on the distribution of these messages, we train our sights on the following three objects: $\mathcal{P}$, $\mathcal{O}$, and

$\mathcal{H} := \texttt{base}(\mathcal{O}^{\perp}) \cdot V + \mathcal{O}$. We make two claims:

1. **About the joint distribution of $(\mathcal{P}, \mathcal{O}, \mathcal{H})$.** It is identical to the distribution produced by the following process:

$$\mathcal{P}, \mathcal{O} \overset{R}{\leftarrow} \texttt{keyGen}(1^{\lambda}); \mathcal{H} \overset{R}{\leftarrow} \{\mathcal{H} \in Gr(n-1, \mathbb{F}_q^n) \mid \mathcal{O} \subseteq \mathcal{H}\}$$

2. **About the results to the signing queries.** All signatures are i.i.d., in particular with the distribution given by this process:

$$C \overset{R}{\leftarrow} \{C \text{ coset of } \mathcal{O}, C \not\subset \mathcal{H}, \mathcal{P} \text{ is of full rank on } C\}, \sigma \leftarrow (\mathcal{P}_{|C})^{-1}(H(m))$$

Now, moving on to the actual reduction — this is what we've talked about before:

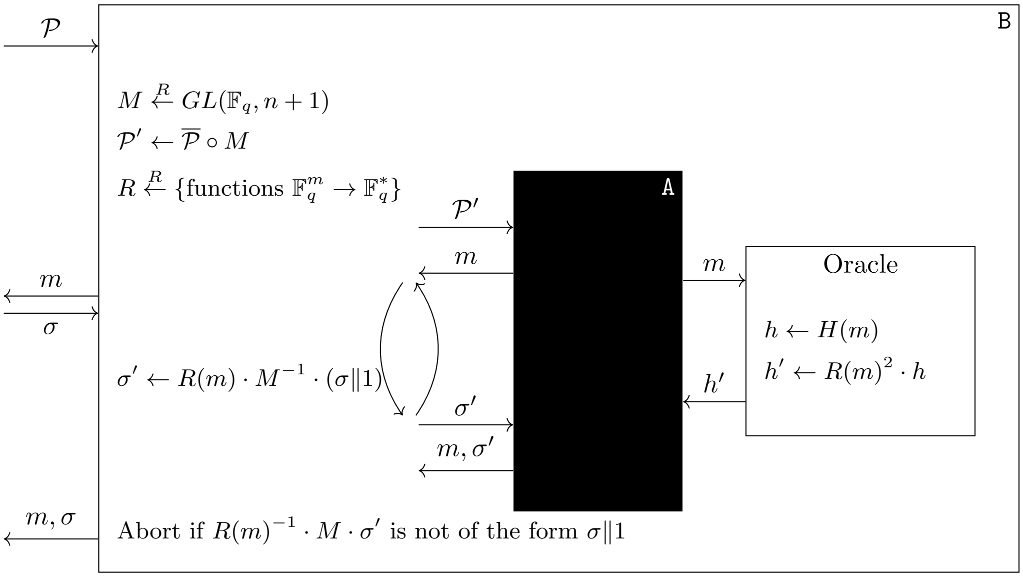

B
$\mathcal{P}$
$M \overset{R}{\leftarrow} GL(\mathbb{F}_q, n+1)$
$\mathcal{P}' \leftarrow \overline{\mathcal{P}} \circ M$
$R \overset{R}{\leftarrow} \{\text{functions } \mathbb{F}_q^m \to \mathbb{F}_q^*\}$
A
$\mathcal{P}'$
m
m
Oracle
$h \leftarrow H(m)$
$h' \leftarrow R(m)^2 \cdot h$
m
σ
$\sigma' \leftarrow R(m) \cdot M^{-1} \cdot (\sigma \| 1)$
h'
σ'
m, σ'
m, σ
Abort if $R(m)^{-1} \cdot M \cdot \sigma'$ is not of the form $\sigma \| 1$

Figure 5

(*Only* during the next paragraph, $\mathcal{P}$ and $\mathcal{O}$ refer to the values of those variables in Fig. 5, and not Fig. 4.)

Again we are interested in the distribution of the messages to A, in particular in three objects analogous to the ones from before: $\mathcal{P}'$, $\mathcal{O}' := M^{-1} \cdot (\mathcal{O} \times \{0\})$, and $\mathcal{H}' := M^{-1}(* \| 0)$. About these three objects, we make exactly the same claims as before:

1. **About the joint distribution of $(\mathcal{P}', \mathcal{O}', \mathcal{H}')$.** It is identical to the distribution produced by the following process:

$$\mathcal{P}', \mathcal{O}' \overset{R}{\leftarrow} \texttt{keyGen}(1^{\lambda}); \mathcal{H}' \overset{R}{\leftarrow} \{\mathcal{H} \in Gr(n-1, \mathbb{F}_q^n) \mid \mathcal{O}' \subseteq \mathcal{H}'\}$$

2. **About the results to the signing queries.** All signatures are i.i.d., in particular with the distribution given by this process:

$$C \overset{R}{\leftarrow} \{C \text{ coset of } \mathcal{O}', C \not\subset \mathcal{H}', \mathcal{P}' \text{ is of full rank on } C\}, \sigma \leftarrow (\mathcal{P}'_{|C})^{-1}(H(m))$$

This implies two things.

Statement 1. As we said, with the distribution of messages to A in Fig. 4, there is a non-negligible probability that A outputs a valid forgery. We have seen (claimed) that this is the same distribution of messages as the one in Fig. 5, meaning that there is also a non-negligible probability that A outputs a valid forgery there.

But can B turn this into a valid forgery in the inhomogenous setting? Yes, but this isn't immediately obvious (though I think it's rather intuitive):

Statement 2. There is a non-negligible probability that, in Fig. 5, A returns a valid forgery *outside* $\mathcal{H}'$.

Proof sketch. Again, since Figs. 5 and 4 are the same "from A's perspective", we shift to the Fig. 4. By contradiction, assume that the claim is false. With statement 1, this implies that A will either abort/produce an invalid signature, or, with non-negligible probability, produce a signature in $\mathcal{H}$. Note, however, that whenever A produces a signature in $\mathcal{H}$, C can easily recover an element from V, and so if A can do this consistently, C can use A to efficiently sample V. If this is possible, then this would (with some fiddling) break the MH_q problem, which we assume to be hard. □

So we obtain that, with non-negligible probability, A produces a valid signature outside of $\mathcal{H}'$. In Fig. 5, this means that with non-negligible probability, A will output a signature (m, σ), with σ of the form $M^{-1} \cdot (*\|r)$, with $r \neq 0$. Now, if is a valid forgery, then A has not queried for a signature of m, and thus A may know $H(m) \cdot R(m)^2$ (from the random oracle), but not $H(m)$ or $R(m)$ individually. This implies it is independent from $R(m)$, meaning that B's final signature attempt, $R^{-1}(m) \cdot M \cdot \sigma = R^{-1}(m) \cdot (*\|r)$, has a non-negligible probability of having its last coordinate set to 1, which would mean that B has managed to produce a signature that is valid in the inhomogenous setting. And that's that!

Some other considerations

Regarding loss in advantage. Both reductions have an "intrinsic" (multiplicative) loss of about $1/q$, which, while tolerable, is certainly uncomfortable for the standard $q \approx 2^8$. Worse still, I haven't said much of anything specific about the loss in advantage in the EUF-CMA reduction, since it's not clear how much loss is introduced by the part to do with sampling V. I would guess this is about $1/e$ (so the total would be about $1/qe$), but this is just a hunch.

Regarding the hardness of MH. There is a rather straightforward idea for trying to solve MH, that is, sampling a bunch of points ($\approx q \cdot n \cdot \log(q)$ is enough for the following idea), and checking if there is a hyperplane that does not intersect any of them. With sufficient probability, this would allow you to distinguish the two distributions. However, "checking if there is a hyperplane that does not intersect any of them" is rather nontrivial:

1. It is NP-complete for $q > 2$ — admits a reduction from q-COLORING.
2. It is in P for $q = 2$ — amounts to solving a linear system.

I like to interpret (1) as a suggestion (a rather tenuous one) that MH might be hard. (2) is damning, but:

Regarding the reduction when $q = 2$. It doesn't work, as per the observation above, because MH_q is easy. However, there exists a much easier alternate route. It is based on the fact that any multivariate quadratic $\mathcal{P}$ in $\mathbb{F}_2$ can be written without linear terms, i.e. $\mathcal{P} = \mathcal{F} + c$, where $\mathcal{F}$ is quadratically homogenous and c is constant. An adversary trying to break $\mathsf{EUF\text{-}CMA}$ security of UOV_2 need only recieve a public key $\mathcal{P}$, split it as described above, feed $\mathcal{F}$ to its internal $\mathsf{homogenousUOV}_2$, and, using the ROM, offset the response to all hash queries by $-c$. It is straightforward to check that this works. Essentially, the trick is that (when $q = 2$) the non-quadratic part of public keys does not depend on the input.

Regarding the converse reduction. Can you reduce $\mathsf{homogenousUOV}$ to UOV? Yes. The reduction isn't *trivial*, but it's very straightforward, doesn't run into any issues. Essentially, in this setting, dehomogenizing is far easier than homogenizing.