Signatures à états à partir de Signatures à usage unique

Louis Salvail

La réduction

- Nous construisons $\mathcal{A}$ dans Sig-Forge$_{\mathcal{A},\pi}$ à partir de $\mathcal{A}^*$ dans Sig-Forge$_{\mathcal{A}^*,\pi^*}$.

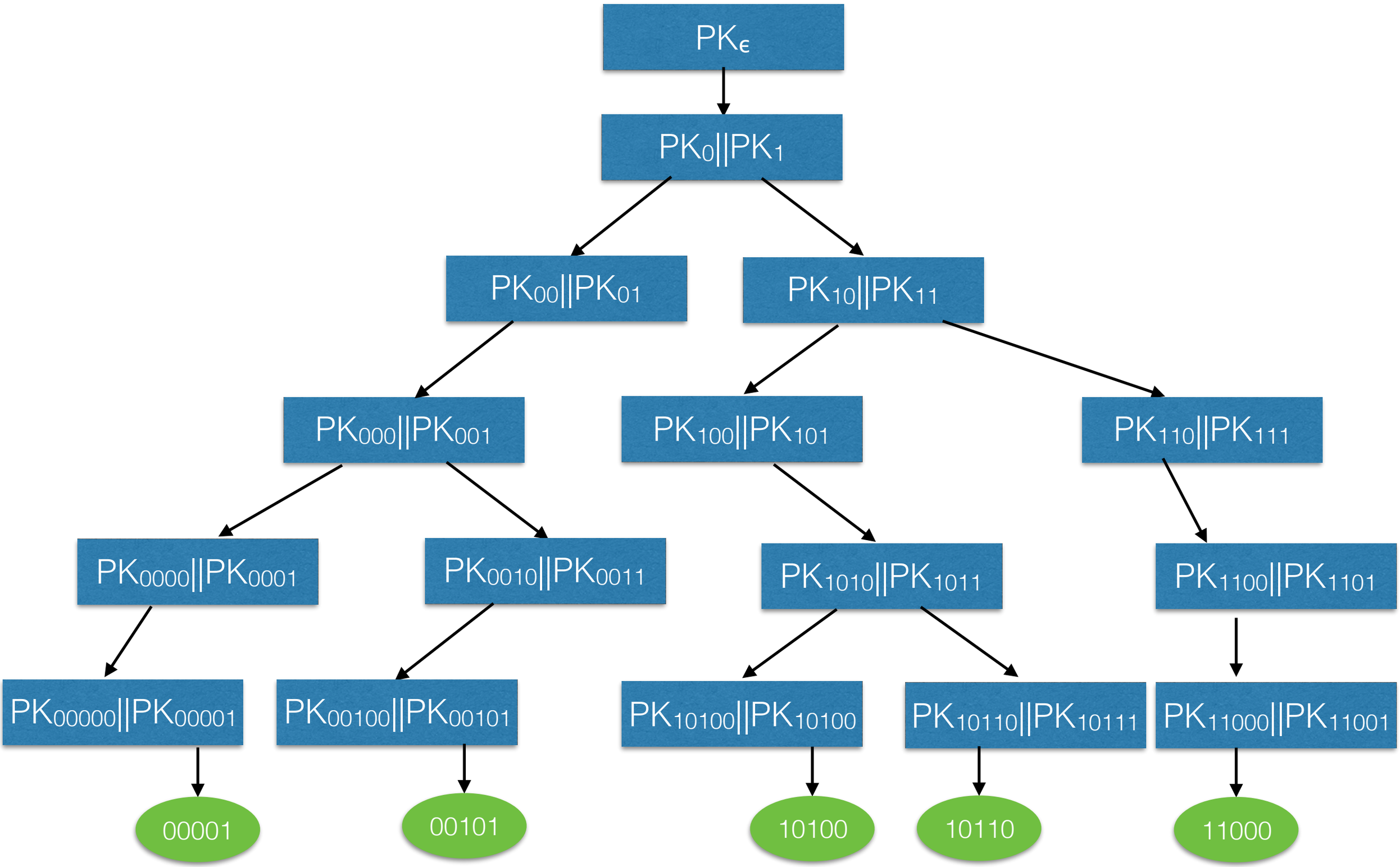
- $\mathcal{A}$ (la réduction) reçoit une clé publique **PK** pour le schéma à usage unique ∏ pour laquelle il doit produire une forgerie.

    - supposons que la clé secrète associée à **PK** est **SK**.

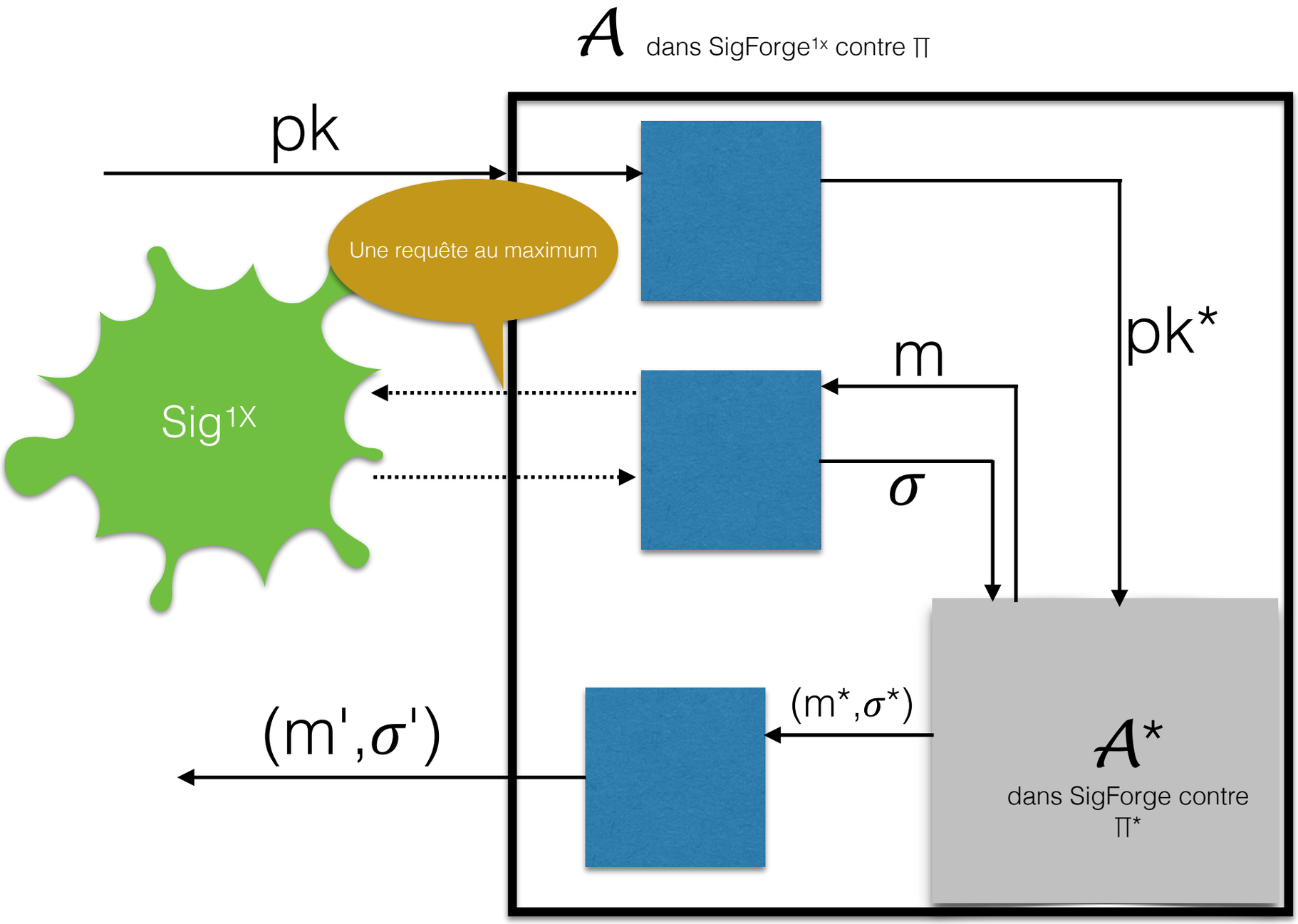
- $\mathcal{A}$ roule $\mathcal{A}^*$ en répondant à ses requêtes de la même façon que le schéma ∏*.

- Après 5 requêtes, l'arbre suivant pourrait représenter la vue résultante de $\mathcal{A}^*$.

Voici un exemple d'un arbre résultant de 5 requêtes faites par $\mathcal{A}^*$



La réduction en gros



La détermination des clés

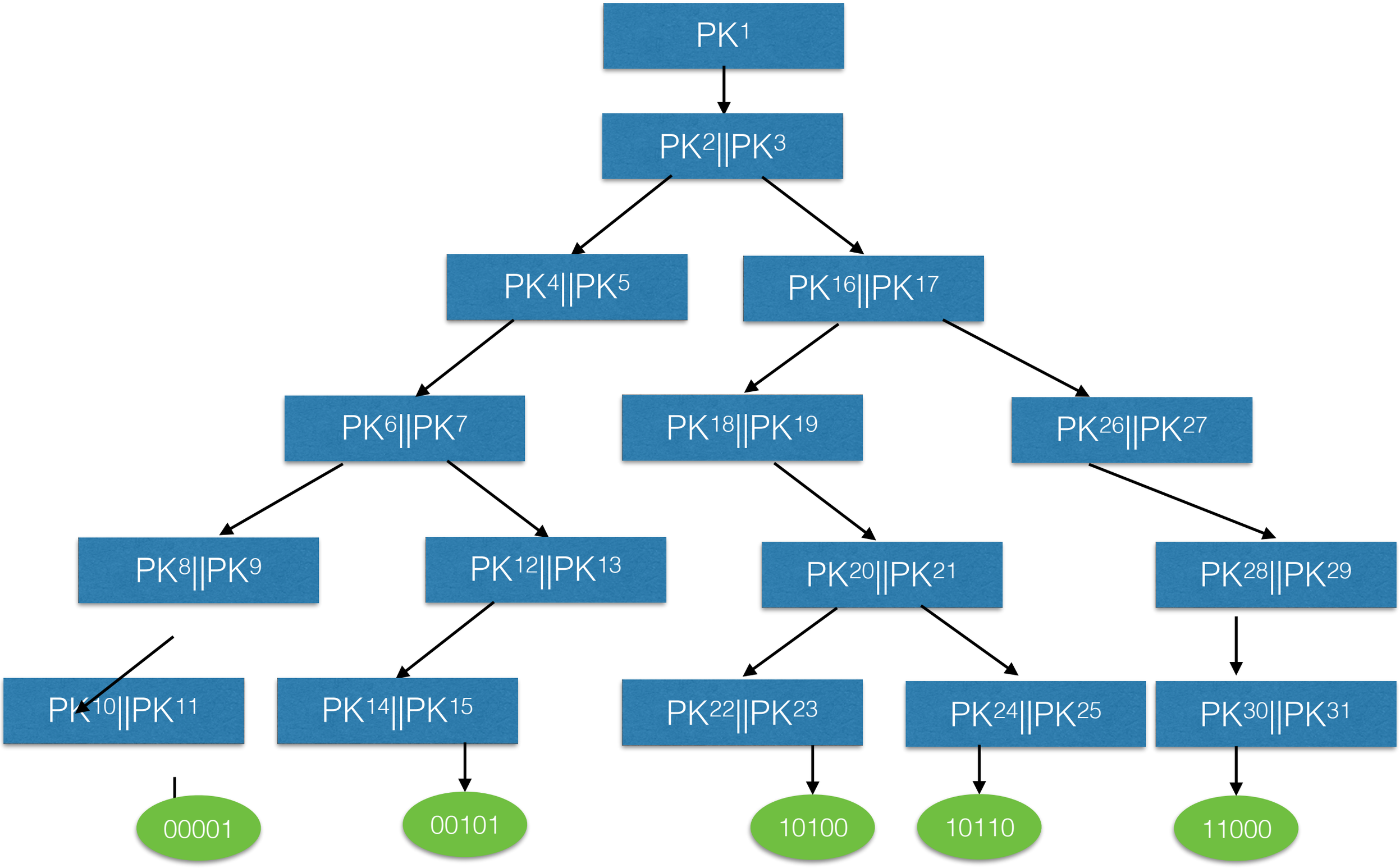
- Dans la réduction de $\mathcal{A}$ contre le schéma de signature à usage unique $\prod$ à $\mathcal{A}^*$ contre le schéma $\prod^*$, les clés à utilisées (où ℓ est une borne supérieure sur le nombre nécessaire) sont:

  - PK^1, PK^2, PK^3, PK^4,..., PK^{ℓ}

  avec, pour i* aléatoire dans {1,.., ℓ}, PK^{i^*}=**PK**, la clé publique en input à la réduction. Les autres clés sont générées par la réduction en utilisant l'algo Gen de $\prod$. Les clés secrètes correspondantes sont utilisées par la réduction pour répondre aux requêtes de $\mathcal{A}^*$.

- Ces clés sont utilisées une à la suite de l'autre lorsque nécessaire en répondant aux requête de $\mathcal{A}^*$. Lorsqu'une signature est demandée pour le schéma à usage unique pour une clé publique produite par la réduction alors la clé secrète correspondante est utilisée pour produire la signature. Si la clé publique est PK^{i^*} alors l'oracle de $Sig_{\mathbf{SK}}(.)$ pour $\prod$ est utilisé pour produire la signature. Il n'y aura qu'une seule requête de ce type puisqu'il n'y a qu'une seule clé de ce type.

- Voici l'arbre résultant des 5 requêtes, si les requêtes sont dans l'ordre: 00001,00101,10100, 10110,11000


PK1
PK2||PK3
PK4||PK5
PK16||PK17
PK6||PK7
PK18||PK19
PK26||PK27
PK8||PK9
PK12||PK13
PK20||PK21
PK28||PK29
PK10||PK11
PK14||PK15
PK22||PK23
PK24||PK25
PK30||PK31
00001
00101
10100
10110
11000

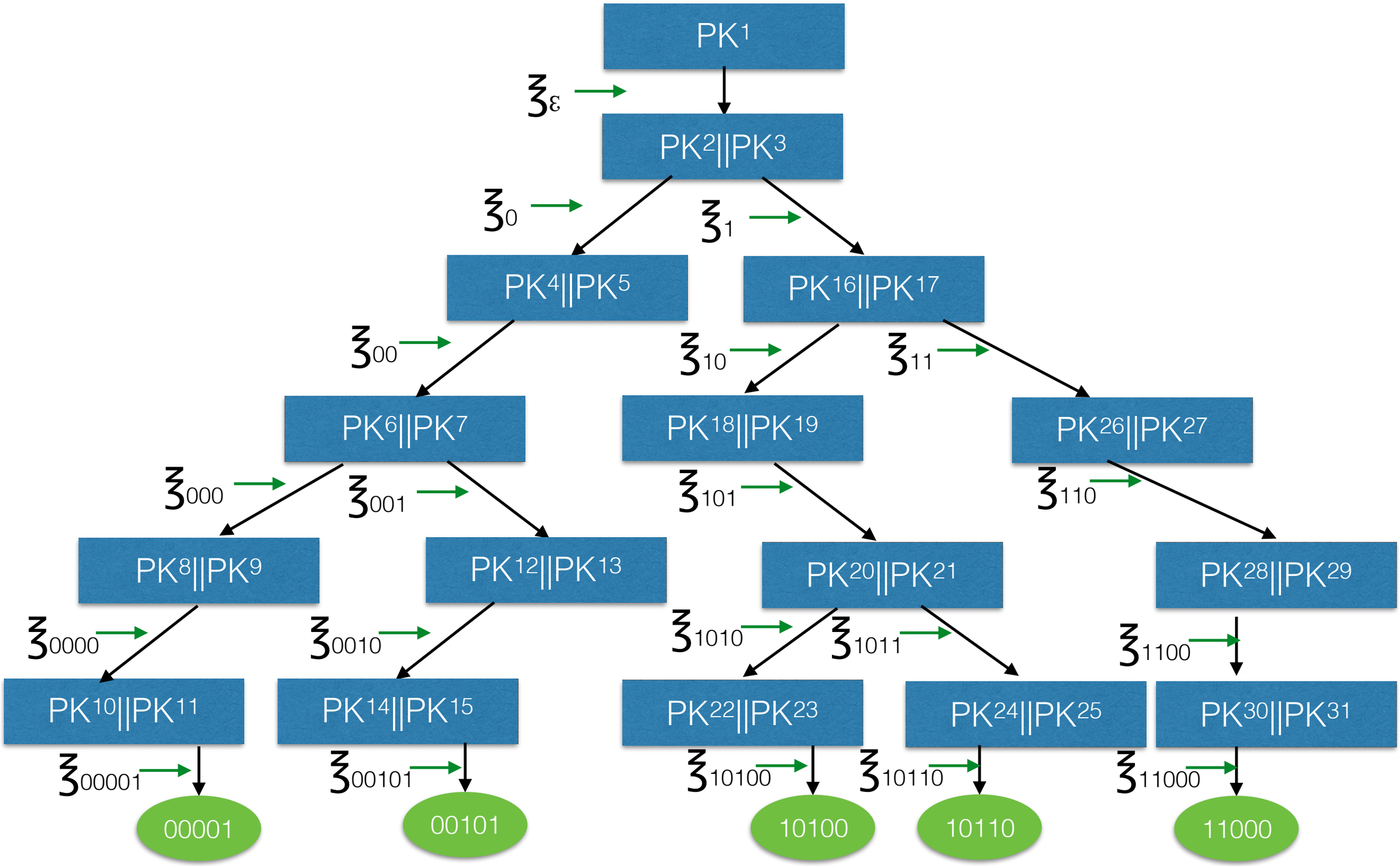
Ajoutons les signatures à usage unique produites par les requêtes

- L'arbre suivant montre l'ensemble de toutes les signatures (paires de clés et messages) produites par les requêtes de signature faites par $\mathcal{A}^*$.

- Nous dénotons par $\sigma_w = Sig_{sk_w}(pk_{w0} || pk_{w1})$ la signature de la paire de clés publiques pk_{w0} et pk_{w1} en utilisant la clé secrète sk_w.

- Aux feuilles (i.e. $w \in \{0,1\}^5$), la signature à usage unique est appliquée au message à signer:

  - $\sigma_w = Sig_{sk_w}(w)$


PK1
ζε
PK2||PK3
ζ0
ζ1
PK4||PK5
PK16||PK17
ζ00
ζ10
ζ11
PK6||PK7
PK18||PK19
PK26||PK27
ζ000
ζ001
ζ101
ζ110
PK8||PK9
PK12||PK13
PK20||PK21
PK28||PK29
ζ0000
ζ0010
ζ1010
ζ1011
ζ1100
PK10||PK11
PK14||PK15
PK22||PK23
PK24||PK25
PK30||PK31
ζ00001
ζ00101
ζ10100
ζ10110
ζ11000
00001
00101
10100
10110
11000

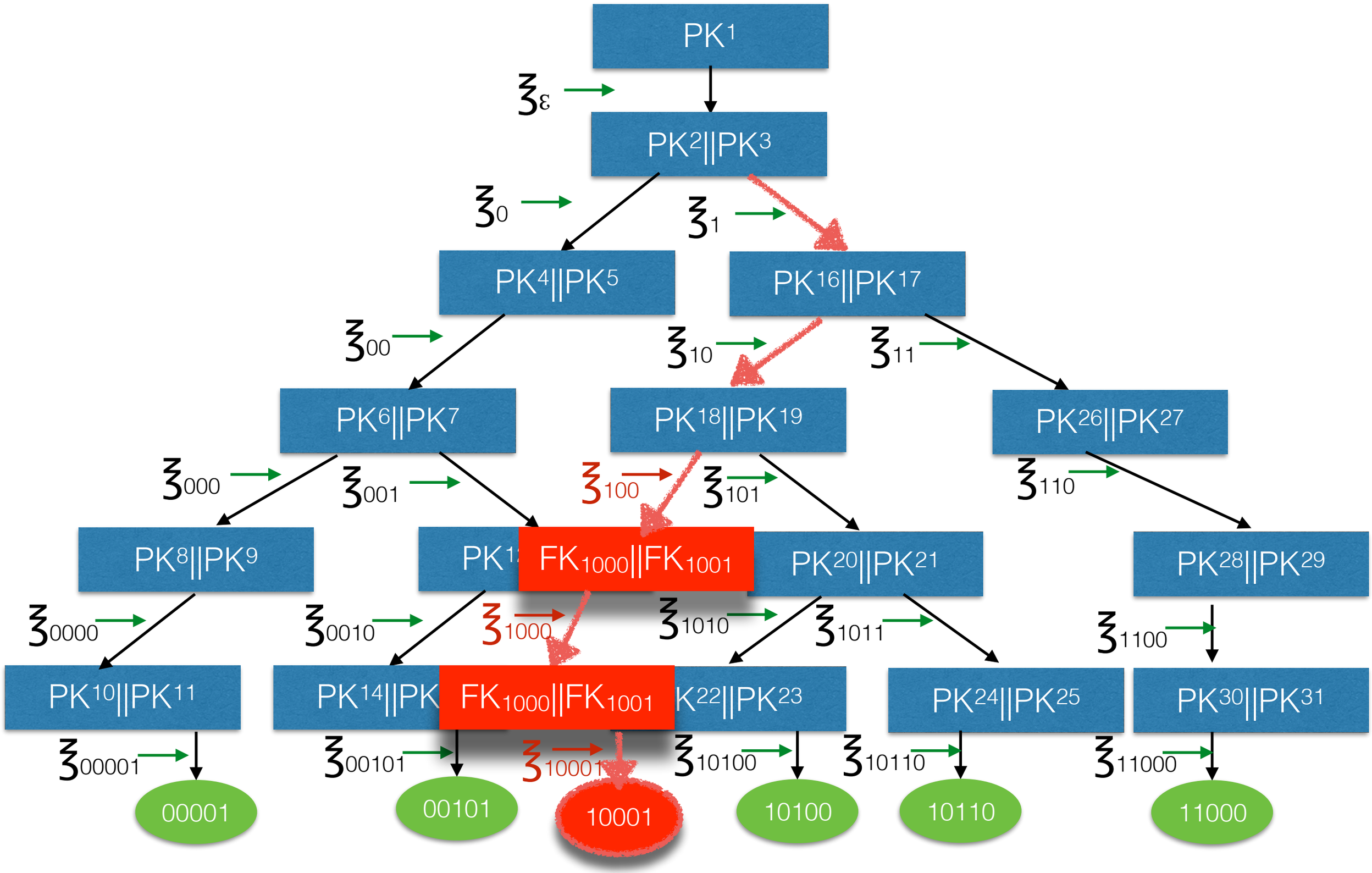
La forgerie

- L'adversaire $\mathcal{A}^*$ contre Π^* voit toutes les signatures ζ_w produites par ses requêtes et indiquées dans l'arbre précédent.

- Une forgerie valide pour $\mathcal{A}^*$doit signer un message qui correspond à une feuille qui n'est pas l'une de celles demandées par ses requêtes.

- En voici une indiquée en rouge sur l'arbre suivant.

Une forgerie de $\mathcal{A}^*$ dans Sig-Forge$_{\mathcal{A}^*,\pi^*}$



Les constituants de la forgerie

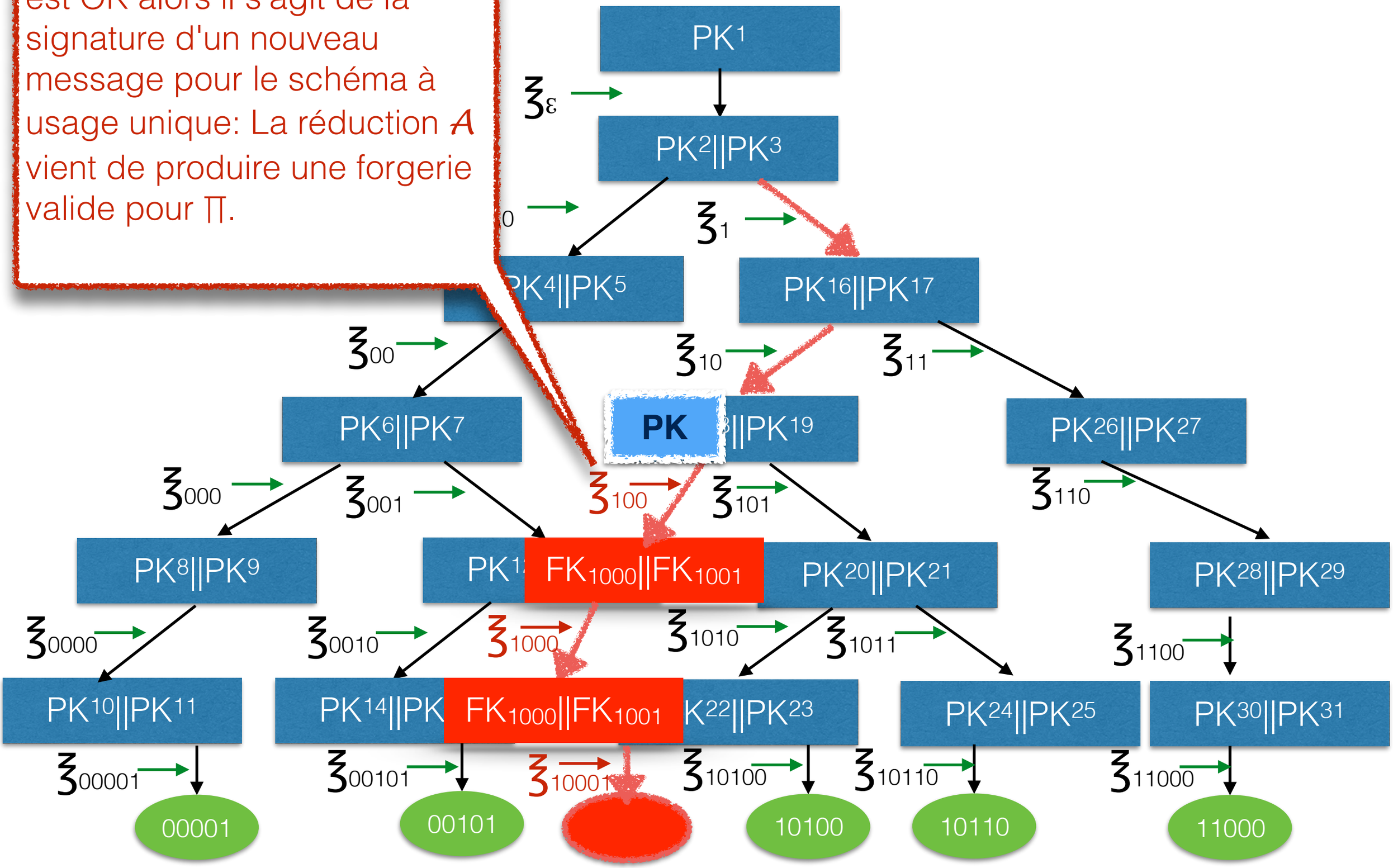
- La forgerie en est une valide pour le message m'=10001 si $\mathcal{A}^*$ produit les signatures à usage unique suivantes:

  - $\{(\sigma_{\varepsilon}, PK^2||PK^3), (\sigma_1, PK^{16}||PK^{17}), (\sigma_{10}, PK^{18}||PK^{19})\}$ qu'il connaît déjà par ses requêtes,

  - $\{(\sigma_{100}, FK_{1000}||FK_{1001}), (\sigma_{1000}, FK_{10000}||FK_{10001}), (\sigma_{10001}, 10001)\}$ qu'il n'a jamais vues. Les clés FK_w sont des clés produites par $\mathcal{A}^*$, **elles ne correspondent pas** aux clés PK^z produites par la réduction. Ces signatures doivent être des forgeries pour le schéma à usage unique.

- Regardons ce qui se passe si, par chance, i*= 18...

Si $Vérif_{PK}(FK_{1000}||FK_{1001}, \zeta_{100})$ est OK alors il s'agit de la signature d'un nouveau message pour le schéma à usage unique: La réduction $\mathcal{A}$ vient de produire une forgerie valide pour Π.



Finalement

- Il est facile de voir que toute forgerie valide de $\mathcal{A}^*$ contient un point où une forgerie de ∏ pour une clé publique choisie par la réduction $\mathcal{A}$. Dans l'exemple précédent, il s'agit de PK^{18}.

- Comme i* est aléatoire, la probabilité qu'il soit égal à cette clé publique choisie par la réduction est au moins$1/\ell$, qui est non-négligeable.

- Si la probabilité de succès de $\mathcal{A}^*$ est non-négligeable alors la probabilité pour $\mathcal{A}$ de gagner dans $Sig\text{-}Forge^{1X}$ est non-négligeable, pour une contradiction.