

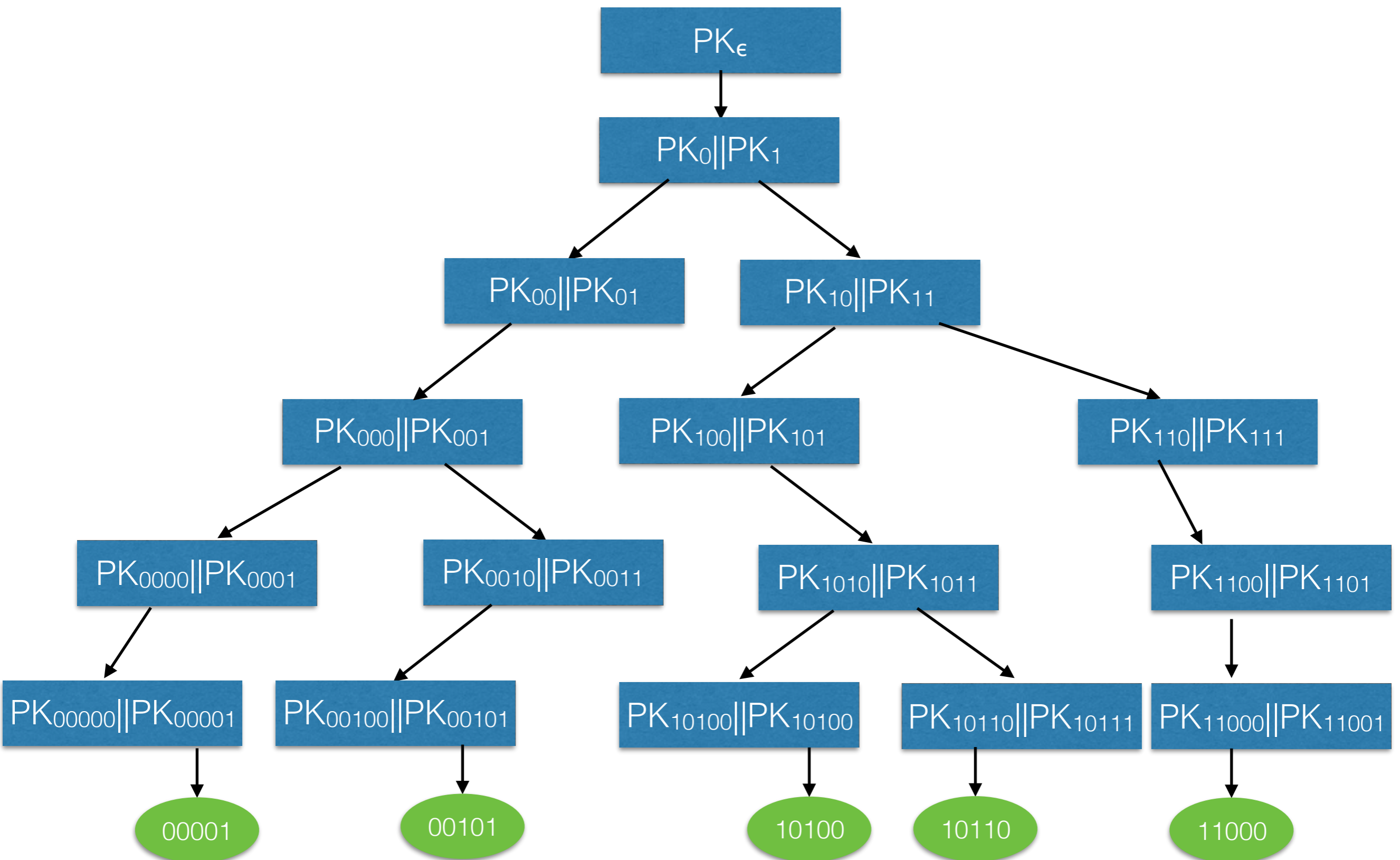
Signature à états à partir de Signature à usage unique

Louis Salvail

La réduction

- Nous construisons A dans $\text{Sig-Forge}_{A,\Pi}$ à partir de A^* dans $\text{Sig-Forge}_{A^*,\Pi^*}$.
- A (la réduction) reçoit une clé publique **PK** pour le schéma à usage unique Π pour laquelle il doit produire une forgerie.
 - supposons que la clé secrète associée à **PK** est **SK**.
- A roule A^* en répondant à ses requêtes de la même façon que le schéma Π^* .
- Après 5 requêtes, l'arbre suivant pourrait représenter la vue résultante de A^* .

Voici un exemple d'un arbre résultant de 5 requêtes faites par A^*



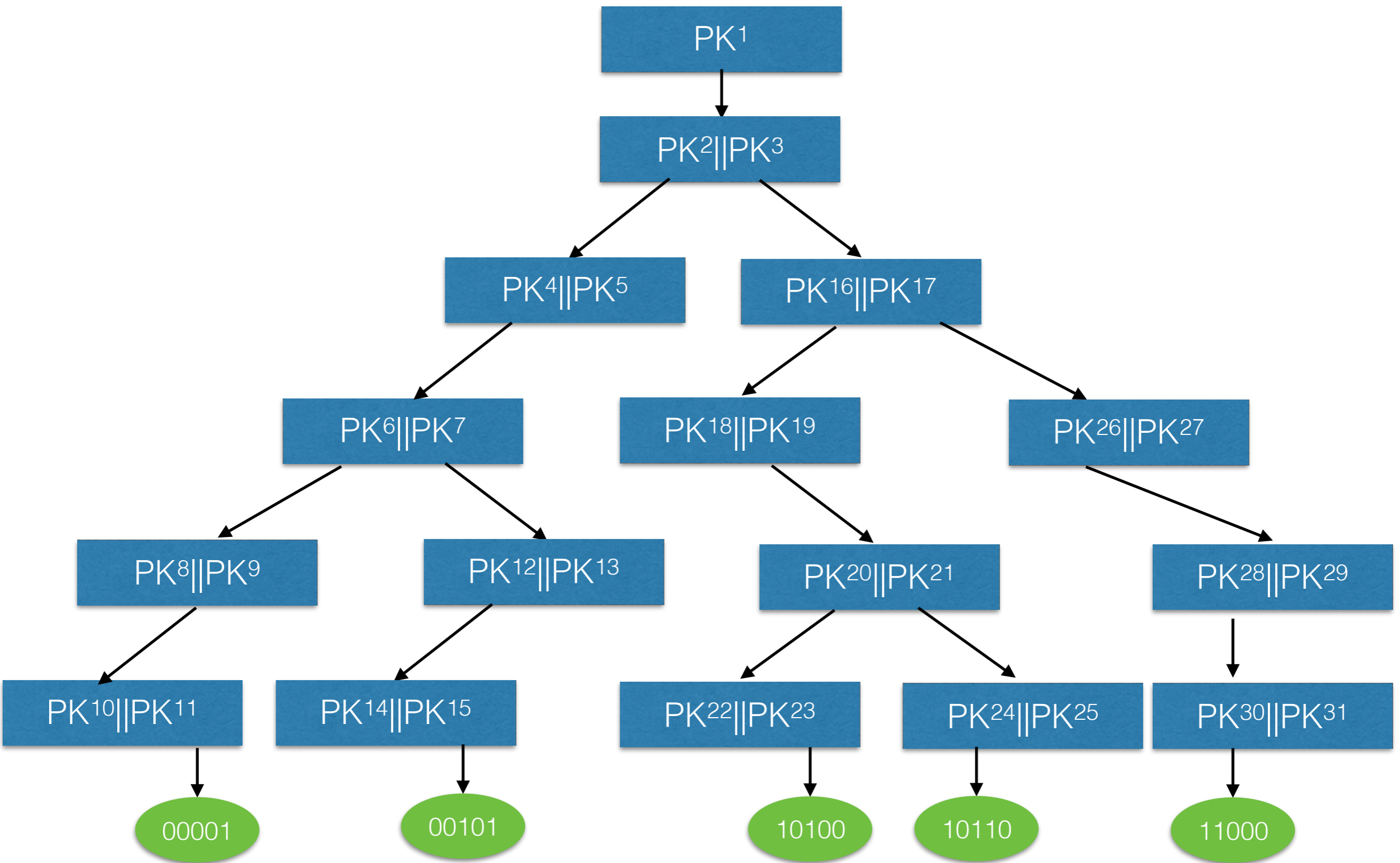
La détermination des clés

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

- $PK^1, PK^2, PK^3, PK^4, \dots, PK^\ell$

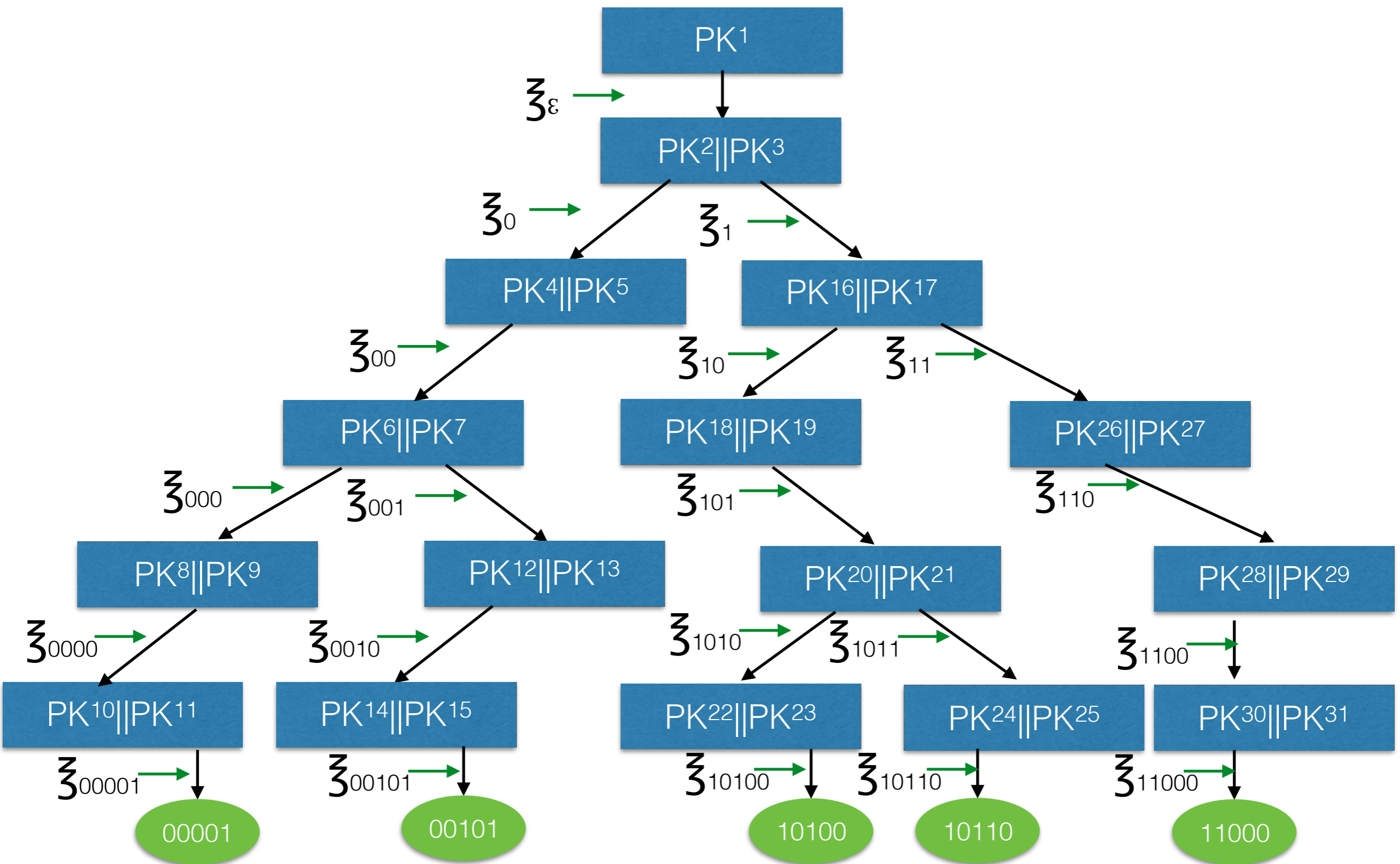
avec, pour i^* aléatoire dans $\{1, \dots, \ell\}$, $PK^{i^*} = \mathbf{PK}$, la clé publique en input à la réduction. Les autres clés sont générées par la réduction en utilisant l'algo Gen de Π . Les clés secrètes correspondantes sont utilisées par la réduction pour répondre aux requêtes de \mathbf{A}^*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

- Ces clés sont utilisées une à la suite de l'autre lorsque nécessaire en répondant aux requête de \mathbf{A}^* . Lorsqu'une signature est demandé 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 $\text{Sig}_{\mathbf{SK}}(\cdot)$ pour Π 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



Ajoutons les signatures à usage unique produites par les requêtes

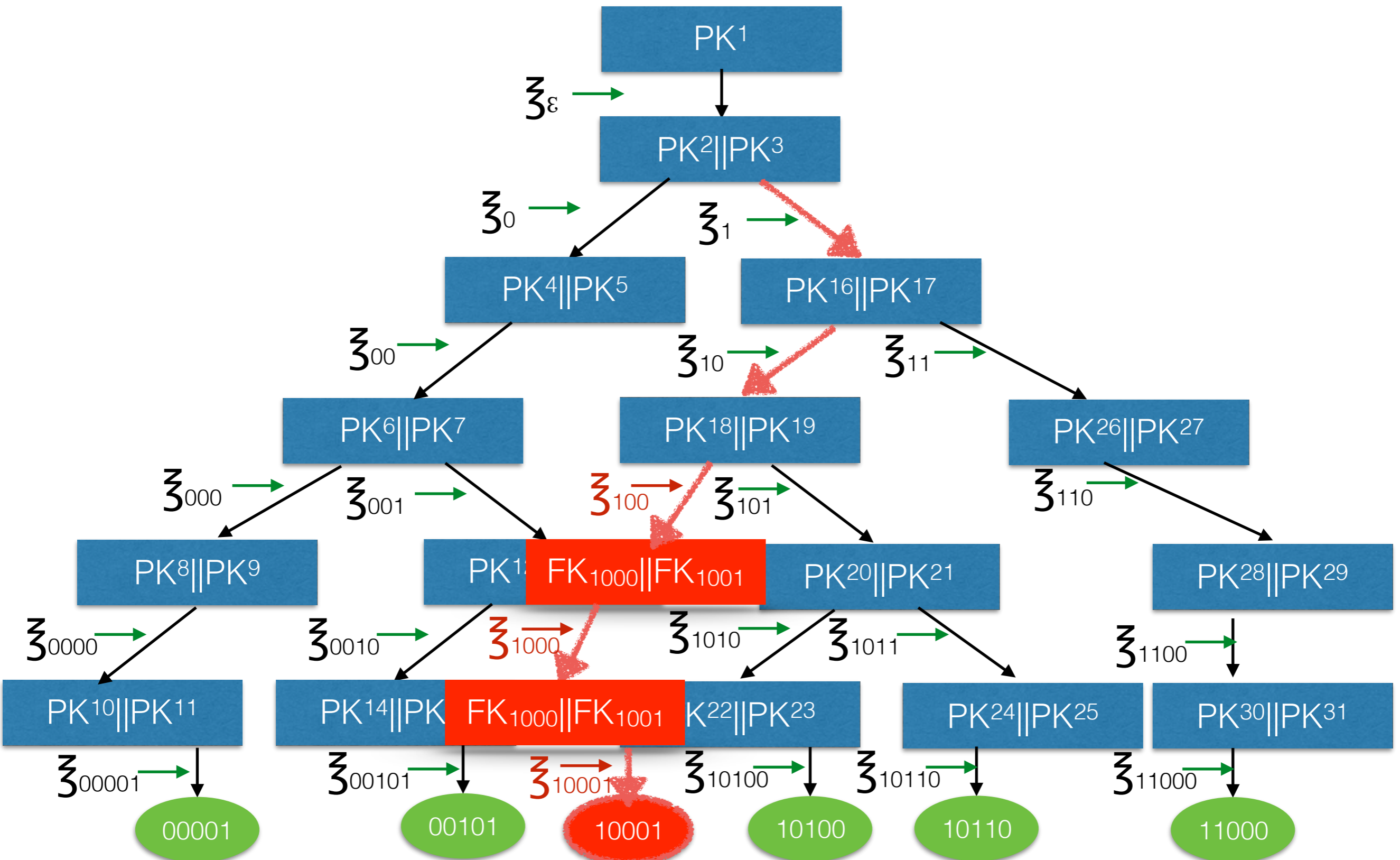
- L'arbre suivant montre l'ensemble de toutes les signatures (paires de clés et messages) produites par les requêtes de signature faites par A^* .
- Nous dénotons par $\zeta_w = \text{Sig}_{sk_w}(pk_{w0} || pk_{w1})$ la signature de la paire de clés publiques pk_{w0} et pk_{w1} en utilisant la clé secrète sk_w .
- Aux feuilles (i.e. $w \in \{0, 1\}^5$), la signature à usage unique est appliquée au message à signer:
 - $\zeta_w = \text{Sig}_{sk_w}(w)$



La forgerie

- L'adversaire A^* contre Π^* voit toutes les signatures \mathfrak{Z}_w produites par ses requêtes et indiquées dans l'arbre précédent.
- Une forgerie valide pour 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 A^* dans $\text{Sig-Forge}_{A^*, \Pi^*}$

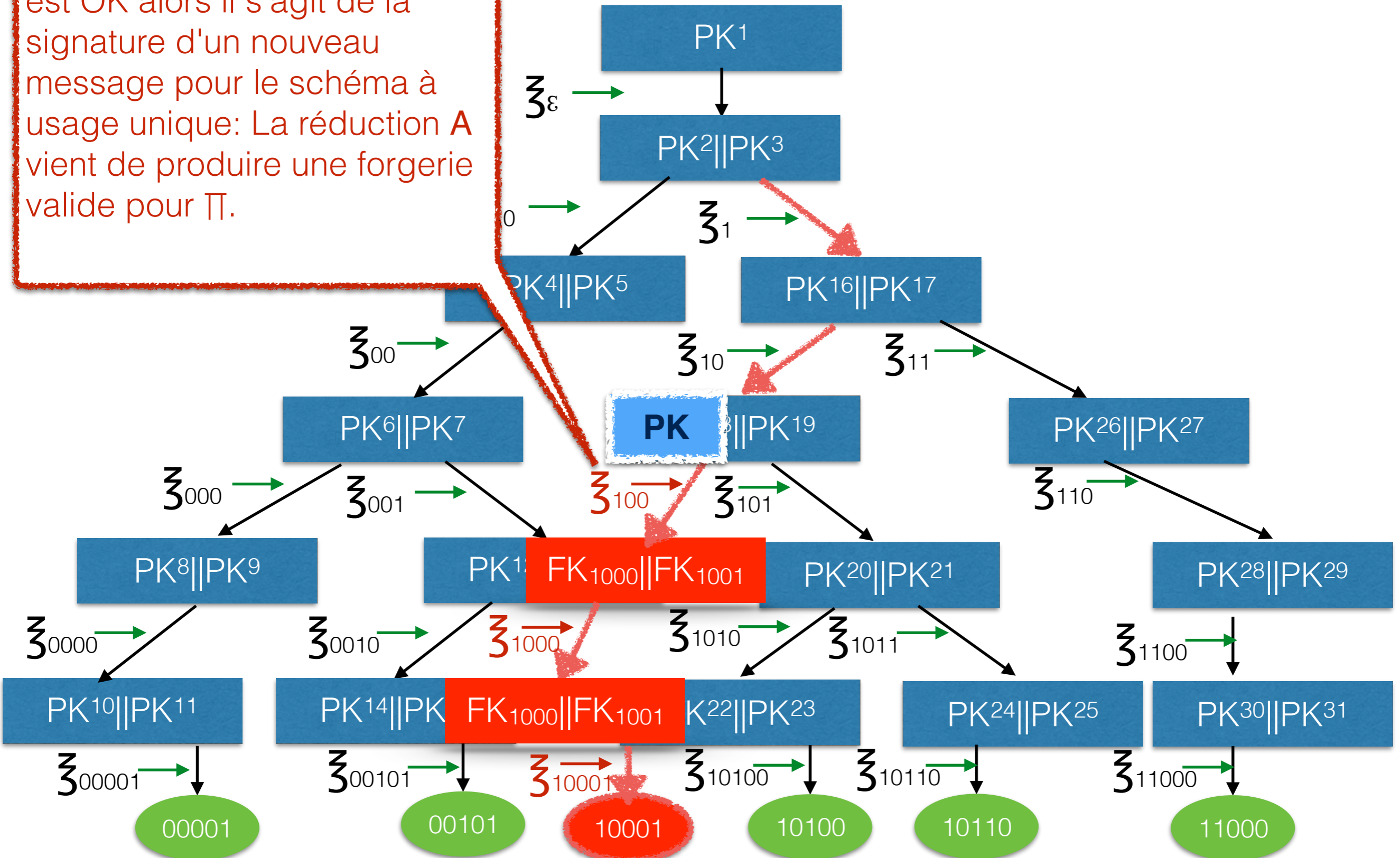


Les constituants de la forgerie

- La forgerie en est une valide pour le message $m'=10001$ si A^* produit les signatures à usage unique suivantes:
 - $\{(\mathfrak{z}_\varepsilon, PK^2 || PK^3), (\mathfrak{z}_1, PK^{16} || PK^{17}), (\mathfrak{z}_{10}, PK^{18} || PK^{19})\}$ qu'il connaît déjà par ses requêtes,
 - $\{(\mathfrak{z}_{100}, FK_{1000} || FK_{1001}), (\mathfrak{z}_{1000}, FK_{10000} || FK_{10001}), (\mathfrak{z}_{10001}, 10001)\}$ qu'il n'a jamais vues. Les clés FK_w sont des clés produites par 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, $i^* = 18...$

$i^* = 18$

Si $\text{Vérif}_{\text{PK}}(\text{FK}_{1000} \parallel \text{FK}_{1001}, \mathfrak{Z}_{100})$ est OK alors il s'agit de la signature d'un nouveau message pour le schéma à usage unique: La réduction A vient de produire une forgerie valide pour Π .



Finalemement

- Il est facile de voir que toute forgerie valide de A^* contient un point où on trouve une forgerie de Π pour une clé publique choisie par la réduction A . Dans l'exemple précédent, il s'agit de PK^{18} .
- Comme i^* est aléatoire, la probabilité qu'il soit égal à l'indice de cette clé publique choisie par la réduction est au moins $1/\ell$, qui est non-négligeable.
- Si la probabilité de succès de A^* est non-négligeable alors la probabilité pour A de gagner dans $\text{Sig-Forge}_{A,\Pi}$ est non-négligeable, pour une contradiction.