

10 Das Merkle-Signatur-Schema (MSS)

Die OTS-Verfahren benötigen für jede neue Signatur ein neues Schlüsselpaar. Eine Lösung* wurde von Ralph Merkle [Merk89] vorgestellt. Merkles Methode verwendet einen binären Hashbaum, um die Gültigkeit vieler OTS-Verifikationsschlüssel auf die Gültigkeit eines einzigen öffentlichen Schlüssels, der Wurzel des Hashbaumes, zurückzuführen.

Initialisierung

Zunächst wird eine Hash-Funktion

$$H: \{0, 1\}^* \rightarrow \{0, 1\}^n$$

und ein Einmal-Signaturverfahren festgelegt. Weiterhin wird* die Anzahl der Signaturen, welche mit einem einzigen Publickey verifizierbar sein sollen, festgelegt $N = 2^h$.

Schlüsselerzeugung

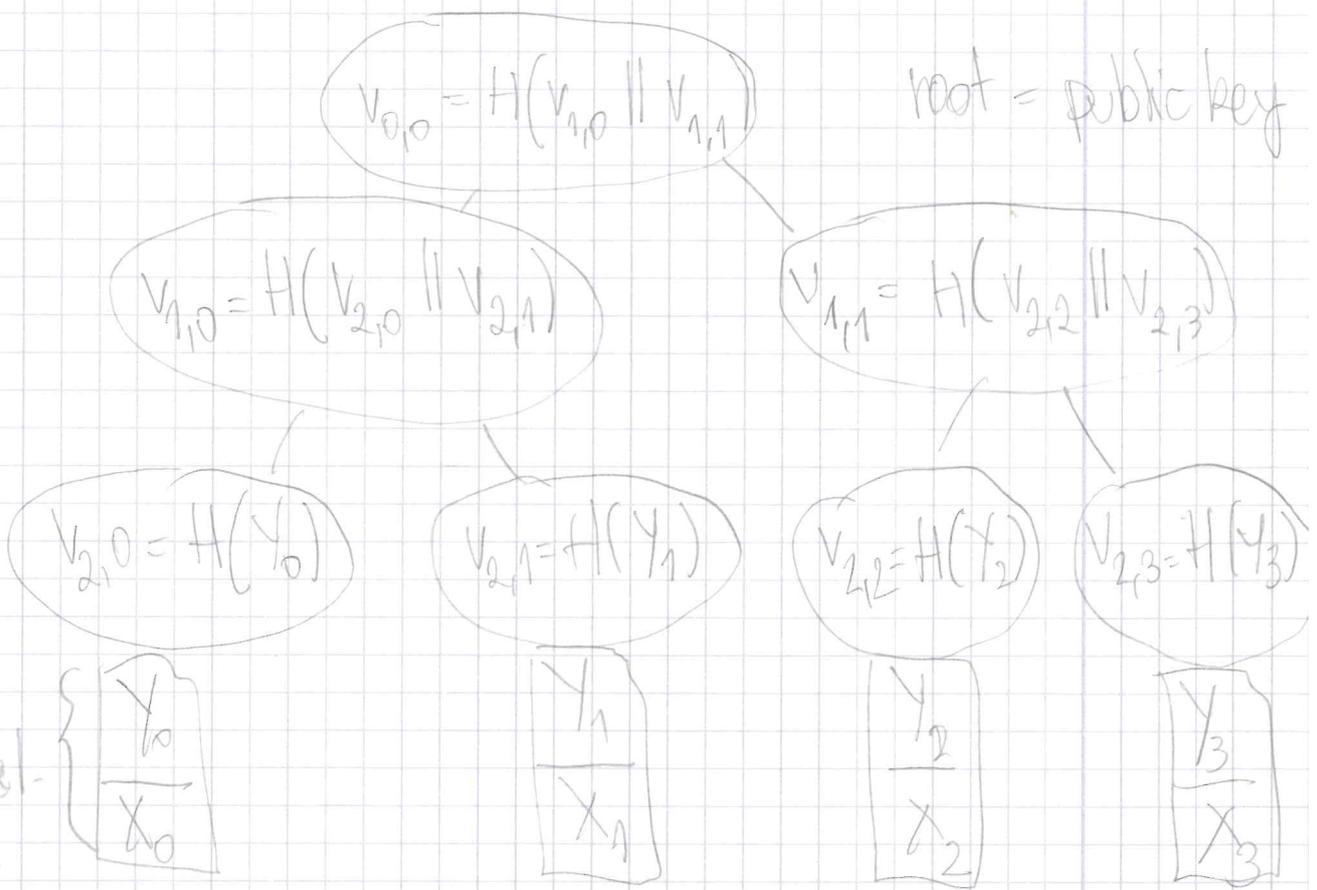
Zunächst berechnet der Signierer passend zum festgelegten OTS N Schlüsselpaare $(x_i, y_i), 0 \leq i < N$. Anschließend wird ein binärer Hashbaum, wie folgt, erzeugt:

* anhand einer natürlichen Zahl h (Baumhöhe)

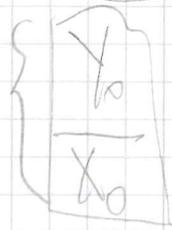
BRUNNEN  *₂ hierfür

PGC(1)

- die Blätter des Baums sind die Hashwerte $H(y_i)$, $0 \leq i < N$ des Verifikationsschlüssels;
- Jeder weitere Knoten ist der Hashwert seiner Kinder $H(k_l || k_r)$, wobei " $k_l || k_r$ " eine Verkettung des linken Kindes " k_l " und des rechten Kindes " k_r " darstellt;
- der geheime Schlüssel ist die Folge (x_0, \dots, x_{N-1}) ;
- der öffentliche Schlüssel ist die Wurzel R (root) des Hashbaumes.



OTS-Schlüssel-Paar



Erzeugung der Signatur

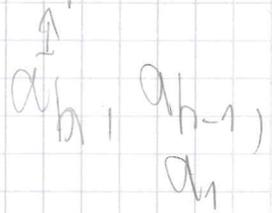
Sei $m \in M$ eine Nachricht und $d = H(m)$ und i der Index des ersten noch nicht verwendeten Signierschlüssels,
→ (STATEFUL)

100(12)

Dann berechnet der Signierer die Einmal-Signatur σ und anschließend wird ~~der~~ einem Authentisierungspfad, welcher die Gültigkeit des Verifikationsschlüssels y_i auf die Gültigkeit des öffentlichen Schlüssels R zurückführt, berechnet.

Der Authentisierungspfad für einen Verifikationsschlüssel y_i ist eine Folge (a_{h-1}, a_h) von Knoten bzw. Hashwerte der Knoten im Hashbaum. Sei $(b_{h-1}, \dots, b_0, b_{\text{gr}})$ der Pfad von Blatt $H(y_i)$ zur Wurzel R , mit $b_h = H(y_i)$ und $b_0 = R$, dann ist der Authentisierungspfad $a_i, h \geq i \geq 1$, der Knoten mit demselben Vater wie b_i .

Bsp.: Sei $i=2$, dann ist der Pfad von Blatt bis zur Wurzel $(v_{2,2}, v_{1,1}, v_{0,0})$ und somit ist der Authentisierungspfad $a_i, h \geq i \geq 1 : (v_{2,3}, v_{1,0})$.



Die Signatur von d ist (im Falle von LD-OTS)

$$\sigma = (i, y_i, \sigma_{\text{ots}}, (a_{h-1}, \dots, a_1)).$$

und im Fall von W-OTS



$$\sigma = (i, \sigma_{\text{ots}}, (a_{h-1}, \dots, a_1)), \text{ da } "y_i = f(\sigma_{\text{ots}})"$$

PQC 13) Verifikation

Der Verifizierer prüft zunächst die OTS. Sollte dies fehlschlagen, wird die Signatur zurückgewiesen, andernfalls wird die Gültigkeit des Verifikationschlüssel y_i überprüft. Hierzu wird der Pfad (p_{h-1}, \dots, p_0) vom i -ten Blatt $H(y_i)$ zur Wurzel, wie folgt, errechnet:

$$p_j = \begin{cases} H(a_{j+1} || p_{j+1}), & \text{if } \lfloor Li/2^{j+1} \rfloor = 1 \pmod 2 \\ H(p_{j+1} || a_{j+1}), & \text{if } \lfloor Li/2^{j+1} \rfloor = 0 \pmod 2, \end{cases}$$

wobei $j = 1, \dots, h$ und $p_h = H(y_i)$ ist. Der Verifizierer akzeptiert die Signatur, wenn $p_h = R$. Bsp.: Sei $i=2$ und $h=2$; dann gilt:

$p_h = R$. Bsp.: Sei $i=2$ und $h=2$; dann gilt:

$$p_0 = H(a_{j+1} || p_{j+1}), \text{ da } \lfloor 2/2^{0+1} \rfloor = 1 \pmod 2$$

