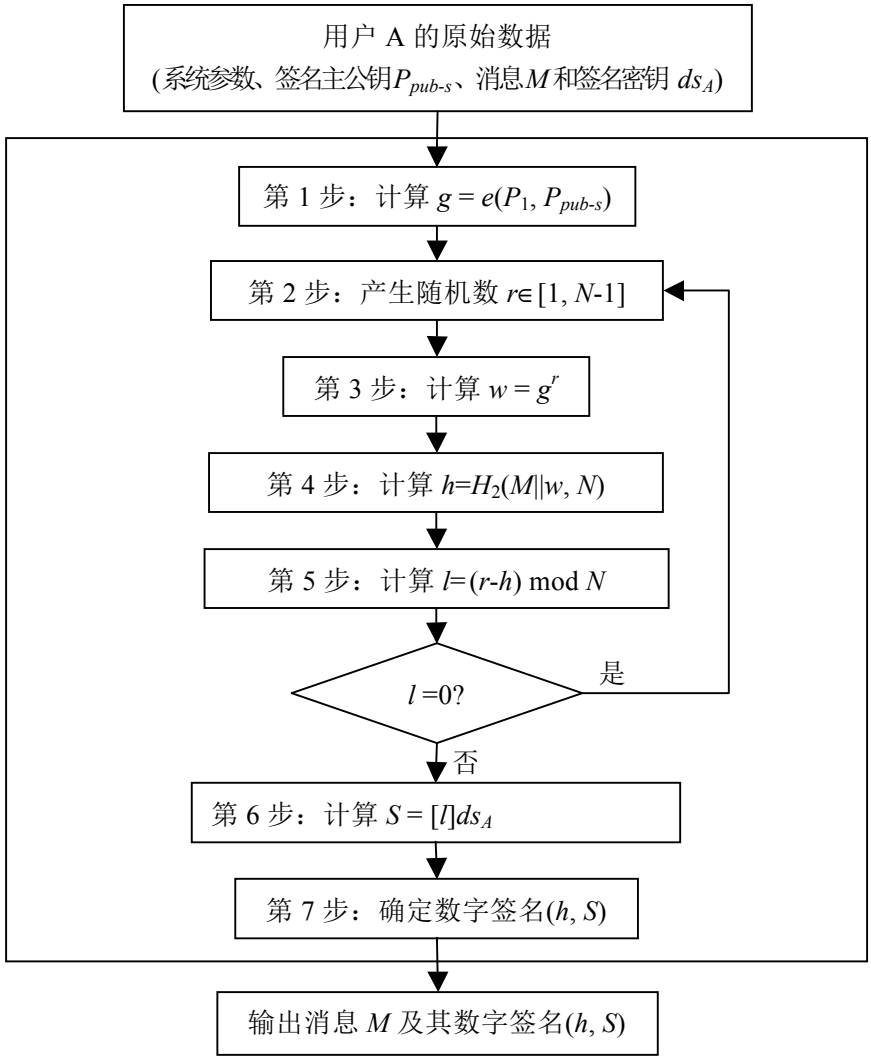


**图1　数字签名生成算法流程**

## 5　数字签名验证算法及流程

### 5.1　数字签名验证算法

为了检验收到的消息 $M'$ 及其数字签名( $h'$, $S'$ )，作为验证者的用户 B 应实现以下运算步骤：

B1：　检验 $h' \in [1, N-1]$ 是否成立，若不成立则验证不通过；

B2：　将 $S'$的数据类型转换为椭圆曲线上的点，检验 $S' \in \mathbb{G}_1$ 是否成立，若不成立则验证不通过；

B3：　计算群 $\mathbb{G}_T$ 中的元素 $g=e(P_1, P_{pub-s})$；

B4：　计算群 $\mathbb{G}_T$ 中的元素 $t=g^{h'}$；

B5：　计算整数 $h_1=H_1(ID_A||hid, N)$；

B6：　计算群 $\mathbb{G}_2$ 中的元素 $P=[h_1]P_2+P_{pub-s}$；

B7：　计算群 $\mathbb{G}_T$ 中的元素 $u = e(S', P)$；

B8：　计算群 $\mathbb{G}_T$ 中的元素 $w' = u \cdot t$，将 $w'$的数据类型转换为比特串；

B9：　计算整数 $h_2 = H_2(M'||w', N)$，检验 $h_2 = h'$ 是否成立，若成立则验证通过；否则验证不通过。

### 5.2　数字签名验证算法流程

数字签名验证算法流程如图2。

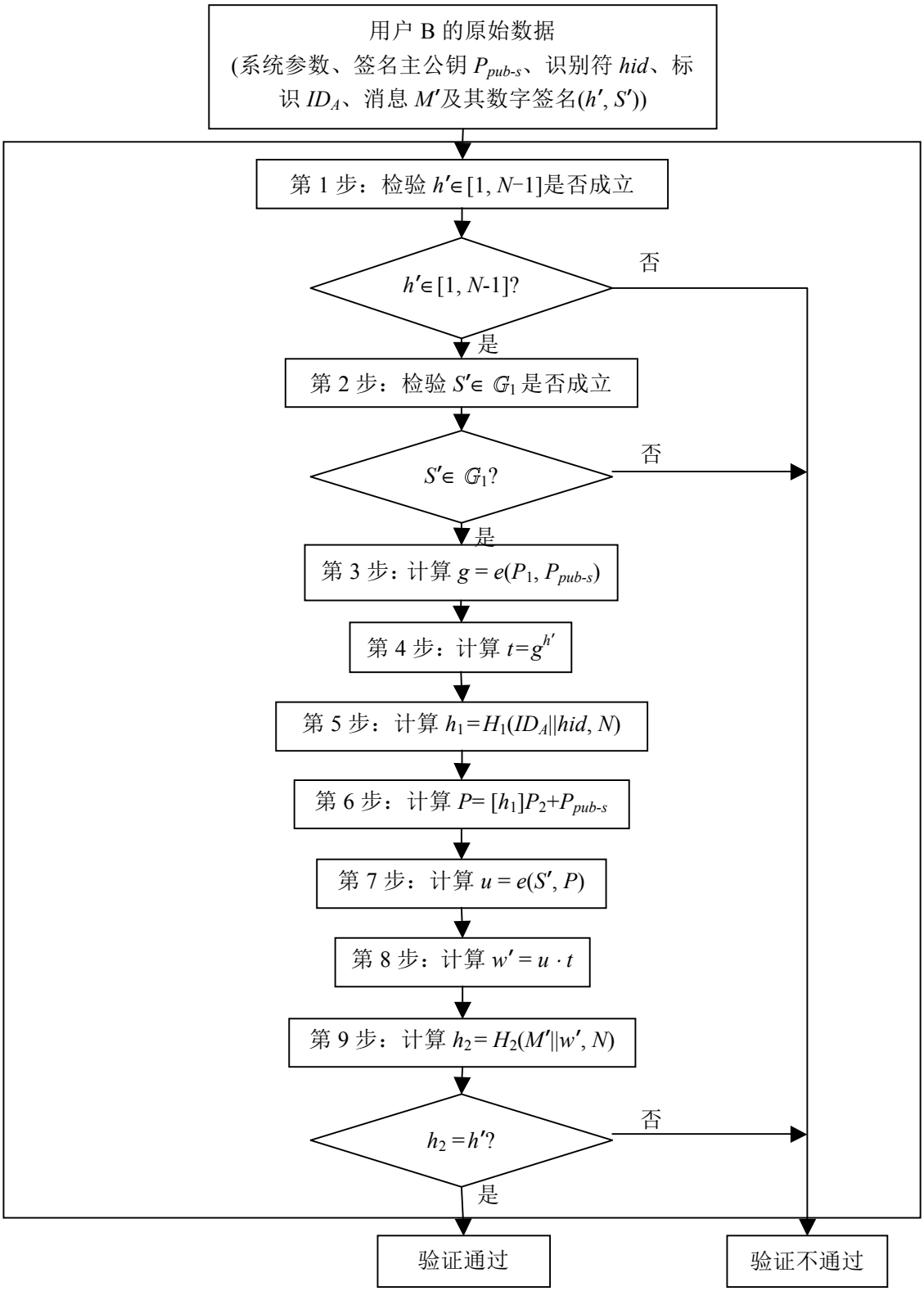


**图2　数字签名验证算法流程**