 3 设计与实现 为了便于描述，我们引入以下几个基本概念： 1. 完全摘要值--指对 ELF 文件的所有数据以及签名相关数据计算出来的摘要值； 2. 不完全摘要值--指对 ELF 文件的一部分重要数据（主要是 ELF 文件头）以及签名相关数据计算出来的摘要值； 3. 完全签名值--指对完全摘要值加密所得到的签名值； 4. 不完全签名值--指对不完全摘要值加密所得到的签名值； 5. 系统验证级别--指系统级的验证级别，它适用于系统中所有的 ELF 文件； 6. 文件验证级别--指单个 ELF 文件的验证级别，它只适用于指定的某个 ELF 文件。 签名相关数据是指原始文件大小、签名者公钥标识 ID、签名算法、签名时间以及签名者基本信息等数据。 3.1 签名策略 对 ELF 文件的签名是通过签名工具完成的，与操作系统核心无关，同时也和平台无关。签名过程完全遵循第二节中所描述的标准和原理。 首先，我们通过 〇1 式计算得到两种摘要值：不完全摘要值（hpart）和完全摘要值（hcomp）。然后再通过 2 式使用签名者私钥（SKsign）加密摘要值，从而得到两种签名值：不完全签名值（spart）和完全签名值（scomp）。 最后，我们将不完全签名值和完全签名值按照固定的格式组合在一起，并放在被签名文件的末尾。如图 3-1 所示（括号中的数字表示该字段所占字节数）。 图 3-1 代码签名过程及签名值存放 