

# Git 与 GitHub 的使用

孙雪 郑海永

2013 年 08 月 11 日

## 目录

<b>1 通过 SSH 代理使用 GitHub</b>	<b>2</b>
1.1 设置 SSH 密钥 . . . . .	2

# 1 通过 SSH 代理使用 GitHub

Git 可以使用四种主要的协议来传输数据：本地传输，SSH 协议，Git 协议和 HTTP 协议。下面简单介绍一下 SSH 如何通过 SSH 代理使用 GitHub。

由于实验室需要，必须通过实验室代理来实现 GitHub 与本地仓库的连接。通过设置 SSH 代理可以实现这一需求，从而完成从本地仓库上传材料到 GitHub 及从 GitHub 克隆仓库到本地等操作。

SSH 为 Secure Shell 的缩写，是建立在应用层和传输层基础上的安全协议，专为远程登录会话和其他网络服务提供安全性的协议，利用 SSH 协议可以有效防止远程管理过程中的信息泄漏问题。

SSH 利用加密的方式可以有效的避免“中间人”截获你和服务器之间的数据传输。所谓“中间人”的攻击方式，就是“中间人”冒充真正的服务器接收你传给服务器的数据，然后再冒充你把数据传给真正的服务器。

SSH 提供了一种基于密匙的安全验证。也就是你必须为自己创建一对密匙，并把公用密匙放在需要访问的服务器上。如果你要连接到 SSH 服务器上，客户端软件就会向服务器发出请求，请求用你的密匙进行安全验证。服务器收到请求之后，先在该服务器上你的主目录下寻找你的公用密匙，然后把它和你发送过来的公用密匙进行比较。如果两个密匙一致，服务器就用公用密匙加密“质询”并把它发送给客户端软件。客户端软件收到“质询”之后就可以用你的私人密匙解密再把它发送给服务器。

下面就来说明 SSH 密匙的设置及如何通过 SSH 代理使用 GitHub。

## 1.1 设置 SSH 密钥

1. 生成密钥。到 ~ 目录下打开终端执行 `ssh-keygen -t rsa`，然后一直按 Enter 键，此时在 ~ 目录下的 `.ssh` 目录下生成了 `id_rsa.pub`。
2. 把公共密钥保存到 GitHub 网站上。到 GitHub 的 Account setting 上

选择 SSH Keys 选项, 点击 Add SSH key, 把 title 写为 `your name@iplouc`。  
把 `id_rsa.pub` 里面的内容复制到 key 中, 保存, 如图1。

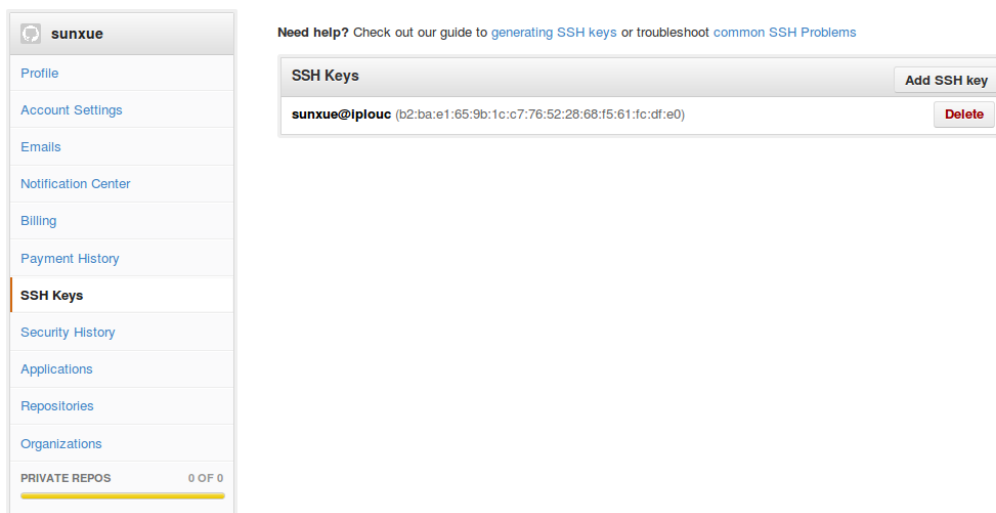


图 1: SSH Keys

如果把本地的 `id_rsa.pub` 里面的内容复制到网页 SSH Key 时没有成功, 提示的错误为如图2: `Key is invalid. Ensure you've copied the file correctly.` 可以尝试在终端输入 `more id_rsa.pub`, 把 `id_rsa.pub` 把内容打印在终端, 如图3, 复制这些内容到网页上的 Add an SSH Key 的 key 中。

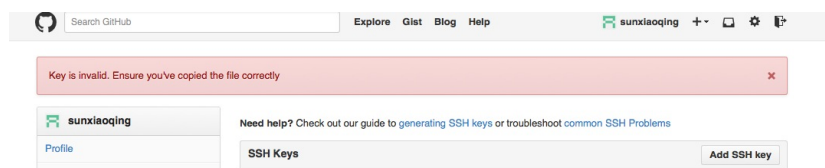


图 2: invalid Key

3. 把密钥加载到 SSH 里。在终端输入 `ssh-add`。

```

[21:11]sunxiaoqing@sunxiaoqingdeMac:~/Documents [1]
$ more ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCsjsji0dDKvyrjGUKGCBrr/CpEa8n6MVEc9uLhQJXd
Rm3tqhCxnwRpzJwzCWCC7vbNDy1uryFF65HwEe2x/5nv8JJmpAe2XmtzV4B5G1be2DYZLqs3t2Er+0aj
AB5AJZZ/wirueAYKqJqNh0+c0y49tgYJ6qUjFtJj fDvdDC0lmdeBhX1kGpS0Hvs2XR09DlUzTumT8rnt
q6JcMp4jZC5XRJE78cvhdTFJiMGJn+A3oasFJA5h+fBL+5tQ2RHk5QgspIiVUzJFC1nsLlvHTbLgS4IC
8c5Ewaf1Ed1wibE4ak9FjAf32C2yH5cHp/UVxT/k7KFFymNFDMS8gjw3uZD sunxiaoqing@sunxiao
qingdeMac.local

```

图 3: invalid Key