Design and Analyze Secure Networked Systems 5

Prof. Edward Chow @ Colorado Univ.

Note by waegaein@github.com

Software Signing

- Provide ways to verify authenticity and integrity of software which are distributed via web.

- GPG

GNU Privacy Guard (GnuPG or GPG) is a tool for secure communication. It can be used to generate public/private key pair.

- PGP

Pretty Good Privacy (PGP) is encryption program that follows OpenPGP standard for encyption/decryption of data.

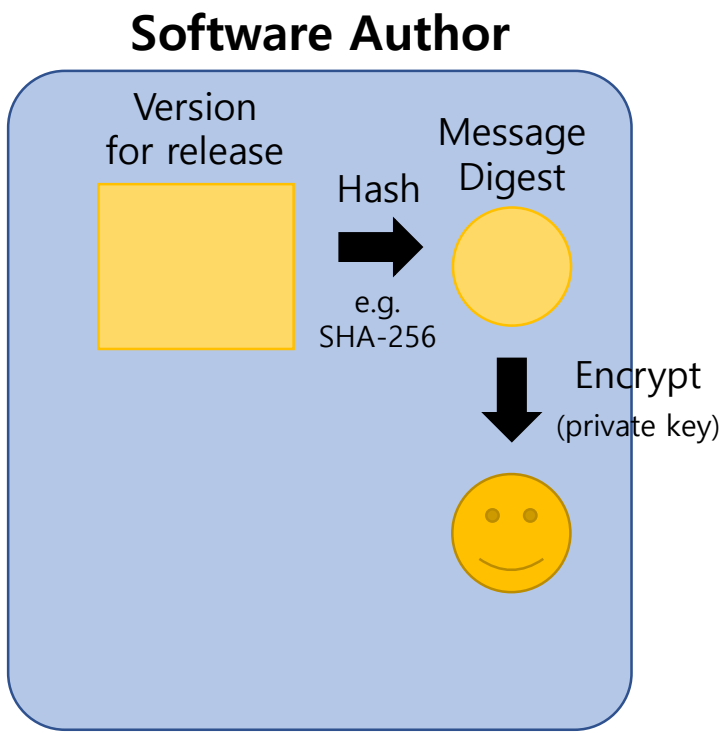
Sign Software

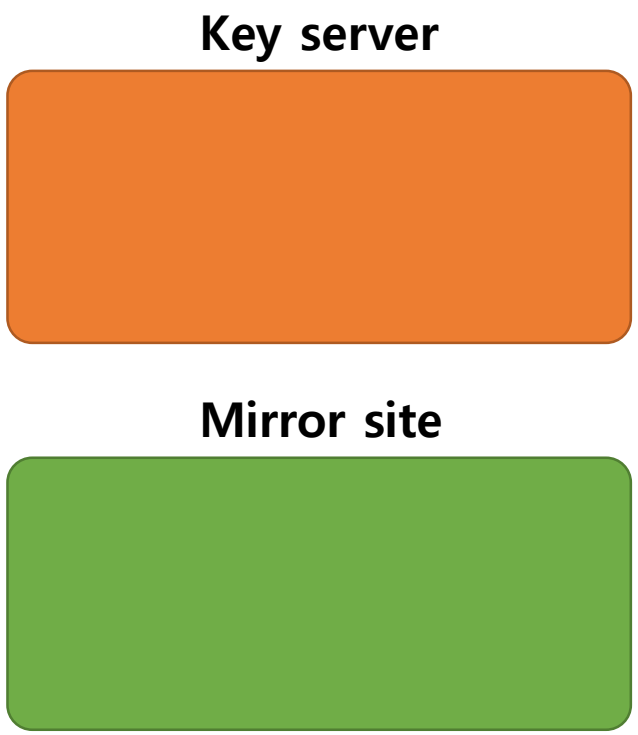
1. Finish a version for release.
2. Generate MD5 and SHA1 message digest of the software.
3. Generate PGP signature of the digest, using private key.
4. Distribute the software with the signature.
5. Distribute the public key, which pairs with the private key used for signing, to key servers.

Sign Software

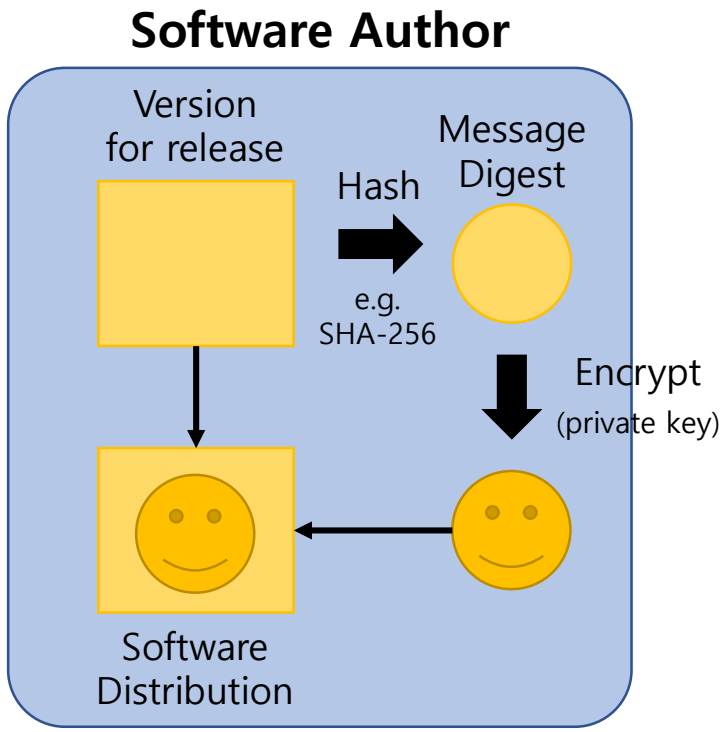
Sign Software

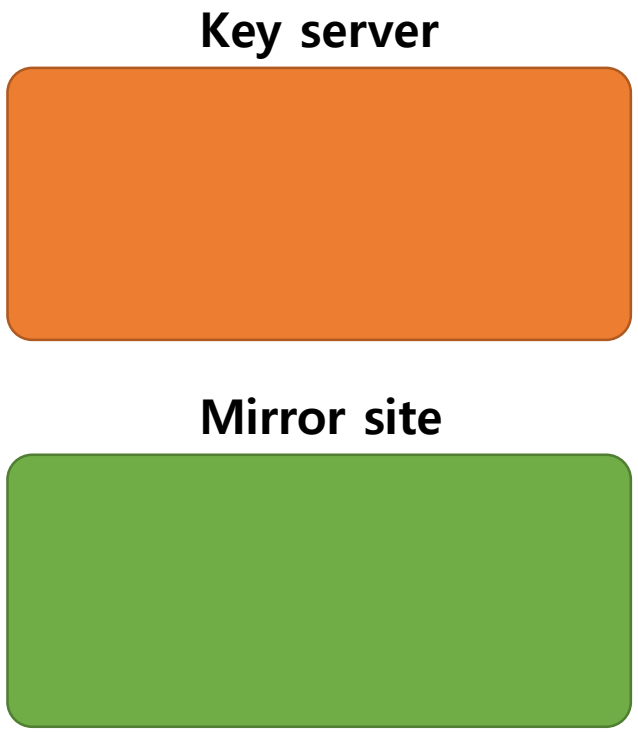
Sign Software



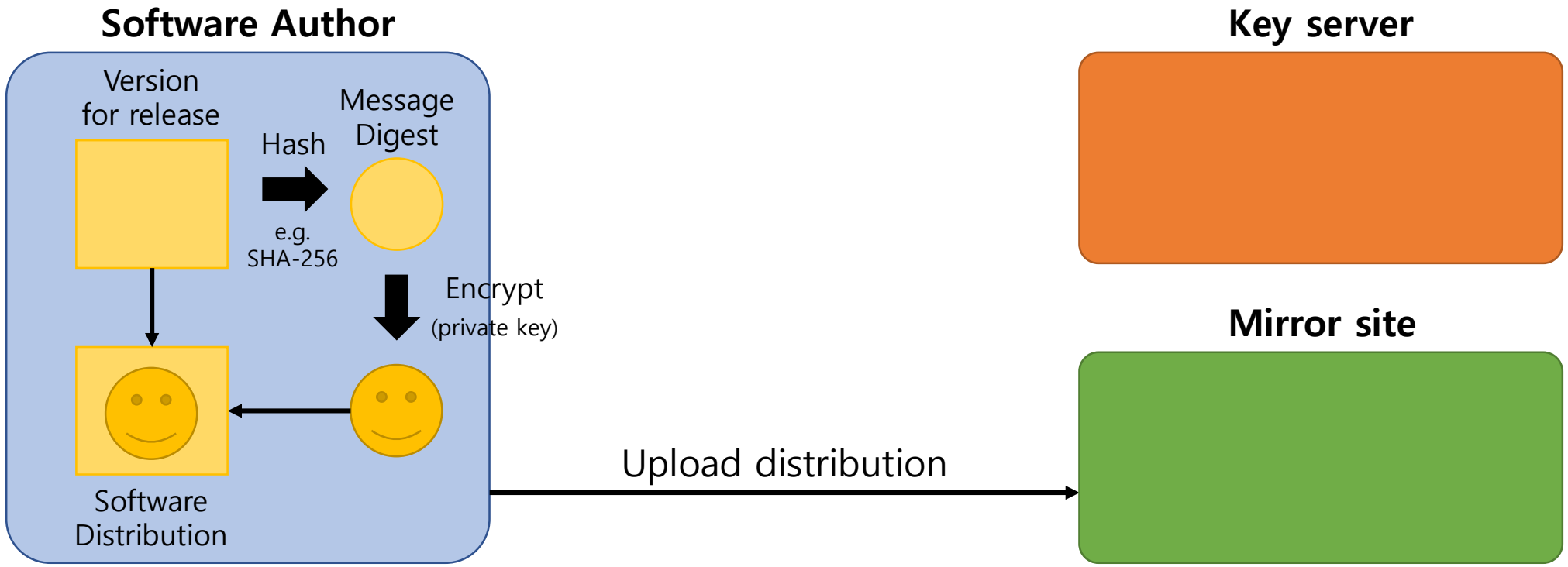


Sign Software

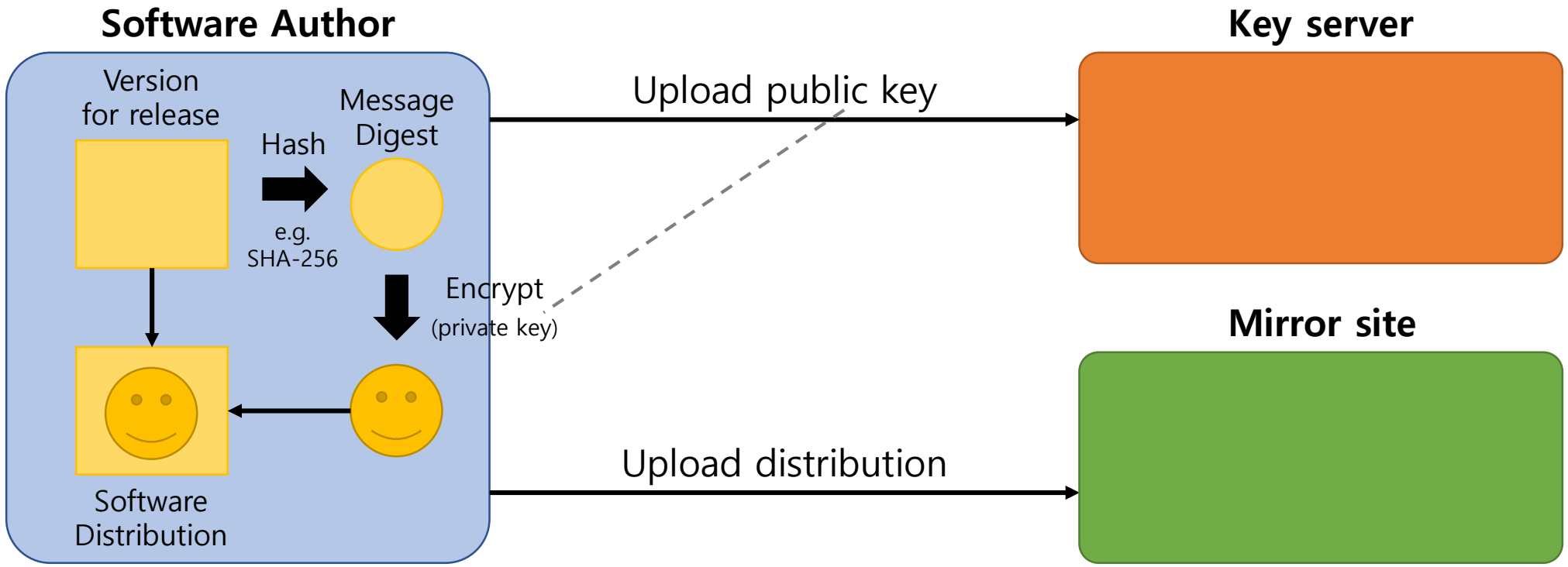




Sign Software



Sign Software

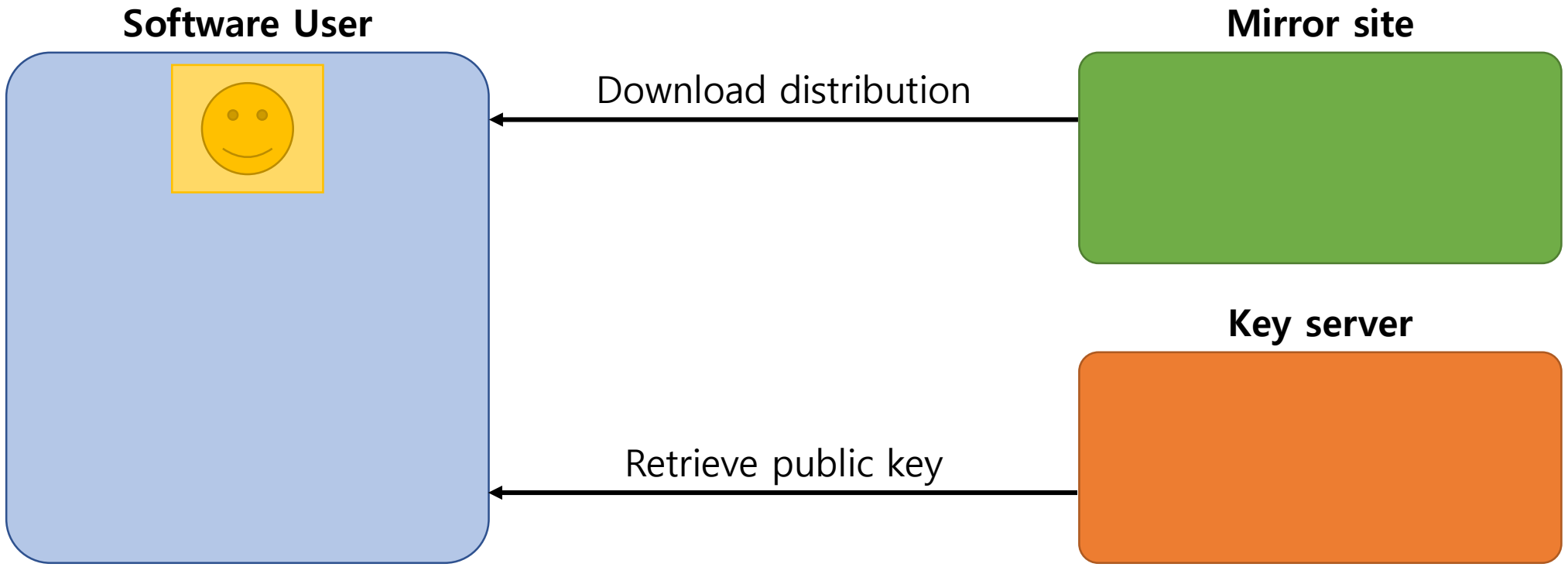


Verify Software

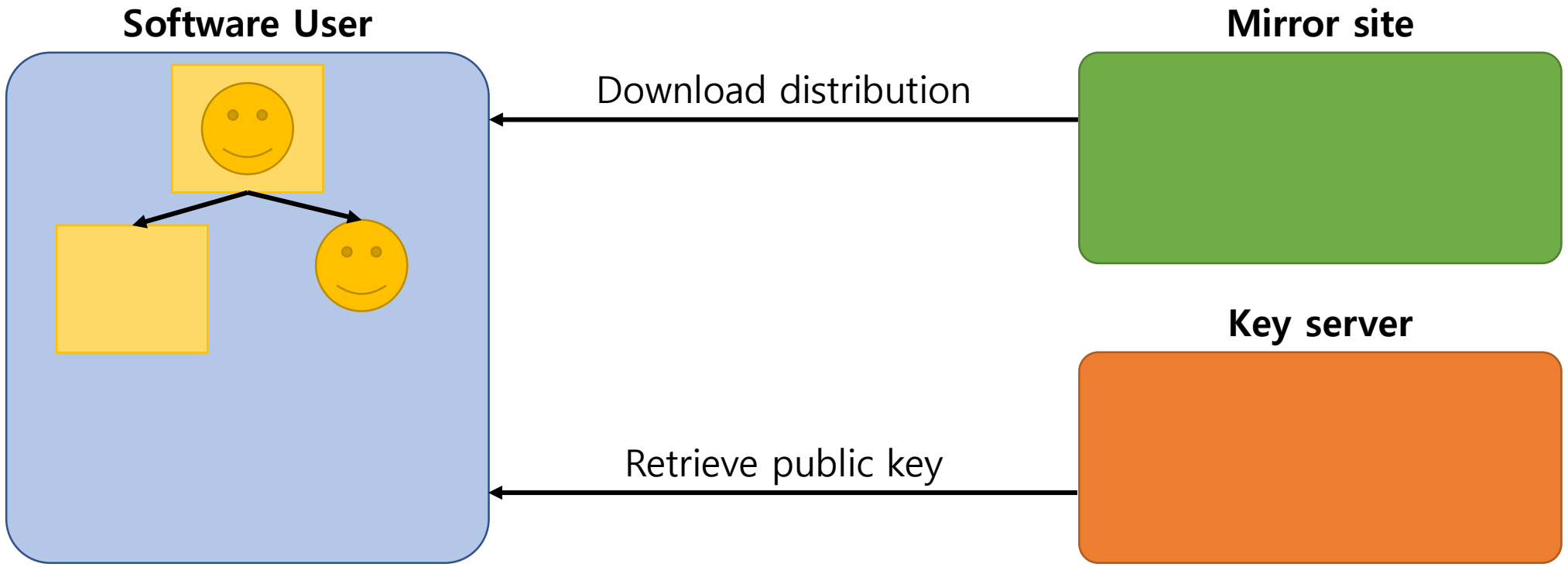
1. Download software and its signature.
2. Retrieve public key from key server.
3. Decrypt the signature into a digest.
4. Generate a digest by hashing the software.
5. If the two digests are identical, the software is verified.
6. If different, the software or signature is considered to be altered.

Verify Software

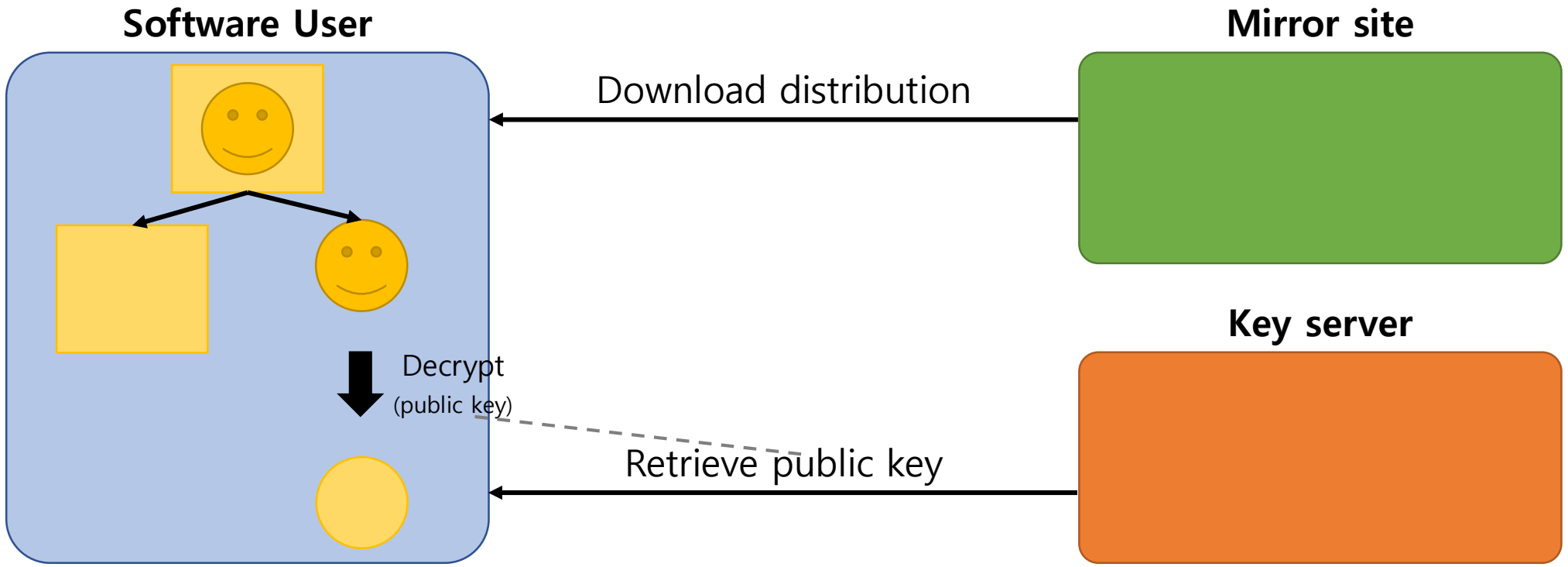
Verify Software



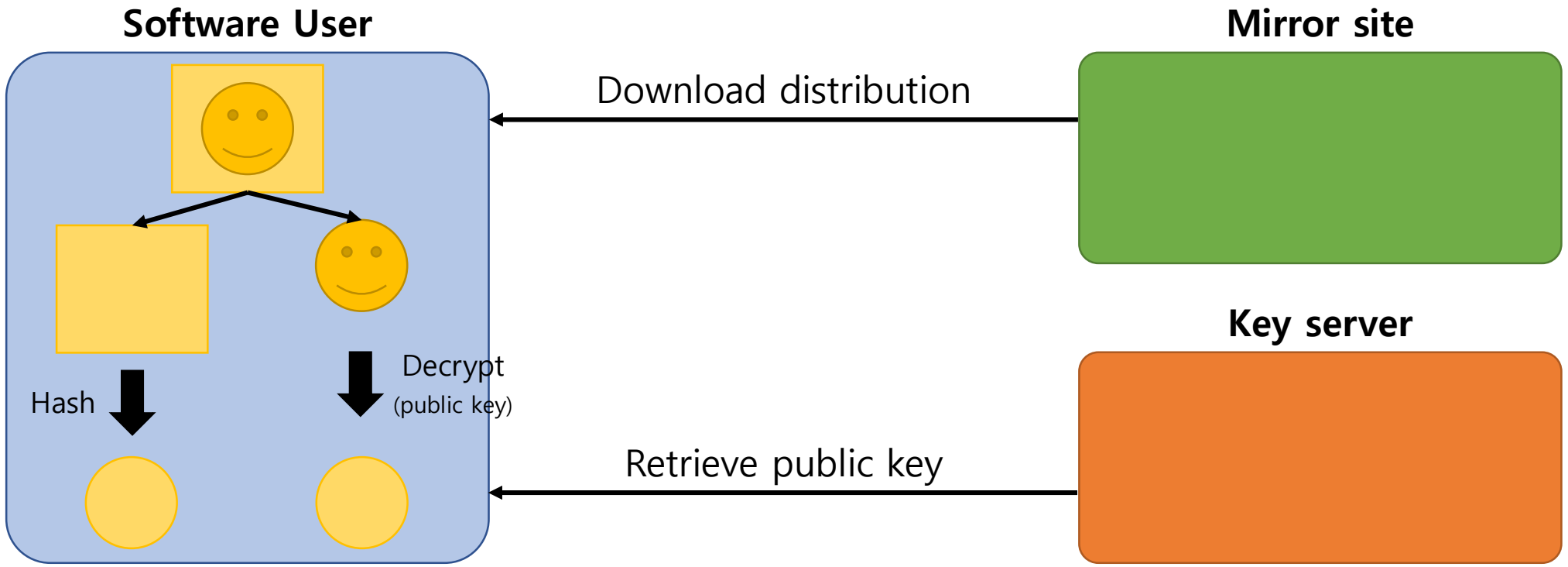
Verify Software



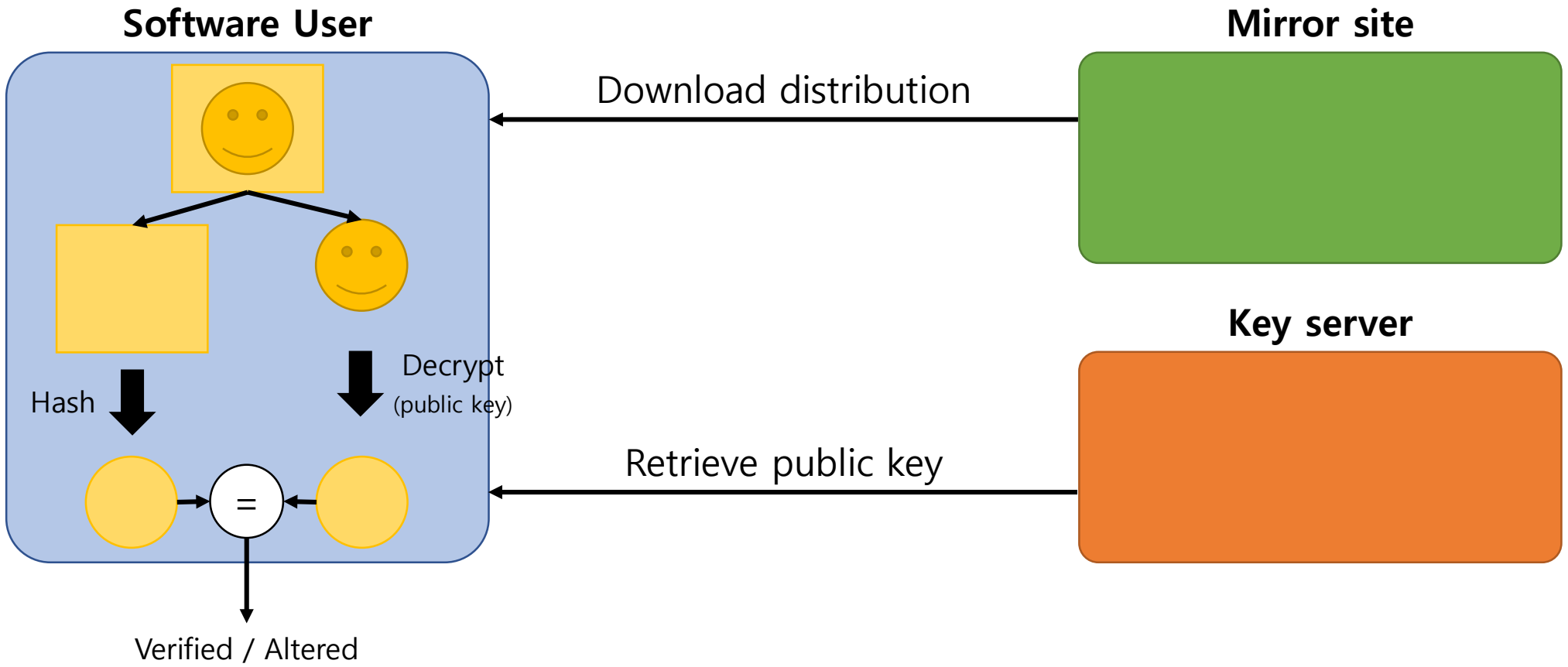
Verify Software



Verify Software



Verify Software



Mirror Sites

- Voluntarily distribute software releases of other organizations to provide faster access.
- Not managed by the original author organizations.
- Encouraged to download bundle from mirrors.
- Encouraged to download hash and signatures only from the original.

PKI vs PGP

- PKI
  - uses CA to vet and bind public keys to user ID.
  - takes longer to register/verify
  - is centralized thus have SPOF.
  - costs fee from CA.
- PGP
  - uses Web of Trust (Key servers) to vet and bind public key to user ID.
  - is hard to revoke keys
  - is distributed.
  - is free.

Misc. How much is encryption safe?

- SHA-1 was cracked by Google 2017.
- … This took the equivalent processing power as **6,500 years of single-CPU** computations and **110 years of single-GPU** computations …
- 110 years of single-GPU
  == 1 year of 110 GPUs
  == 24 hours of 40,150 GPUs
  == 1 hour of 963,600 GPUs
  == 1 minute of 57,816,000 GPUs
  == 10 seconds of 346,896,000 GPUs (**== 9,435,571,200,000 KRW** for only GPUs…)