Authenticated Anonymity by Math

Rüdiger Weis, Bruno Kirschner

OpenTech Summit 2016

Math is your friend

"Trust the math. Encryption is your friend."

- Bruce Schneier, Guardian, 6 September 2013.

ECC

- Embedded Systems
- Personal Devices

Be aware of quantum computing.

Simple blind signature scheme

How to spread a good idea?

Make it simple to . . .

- understand.
- implement.

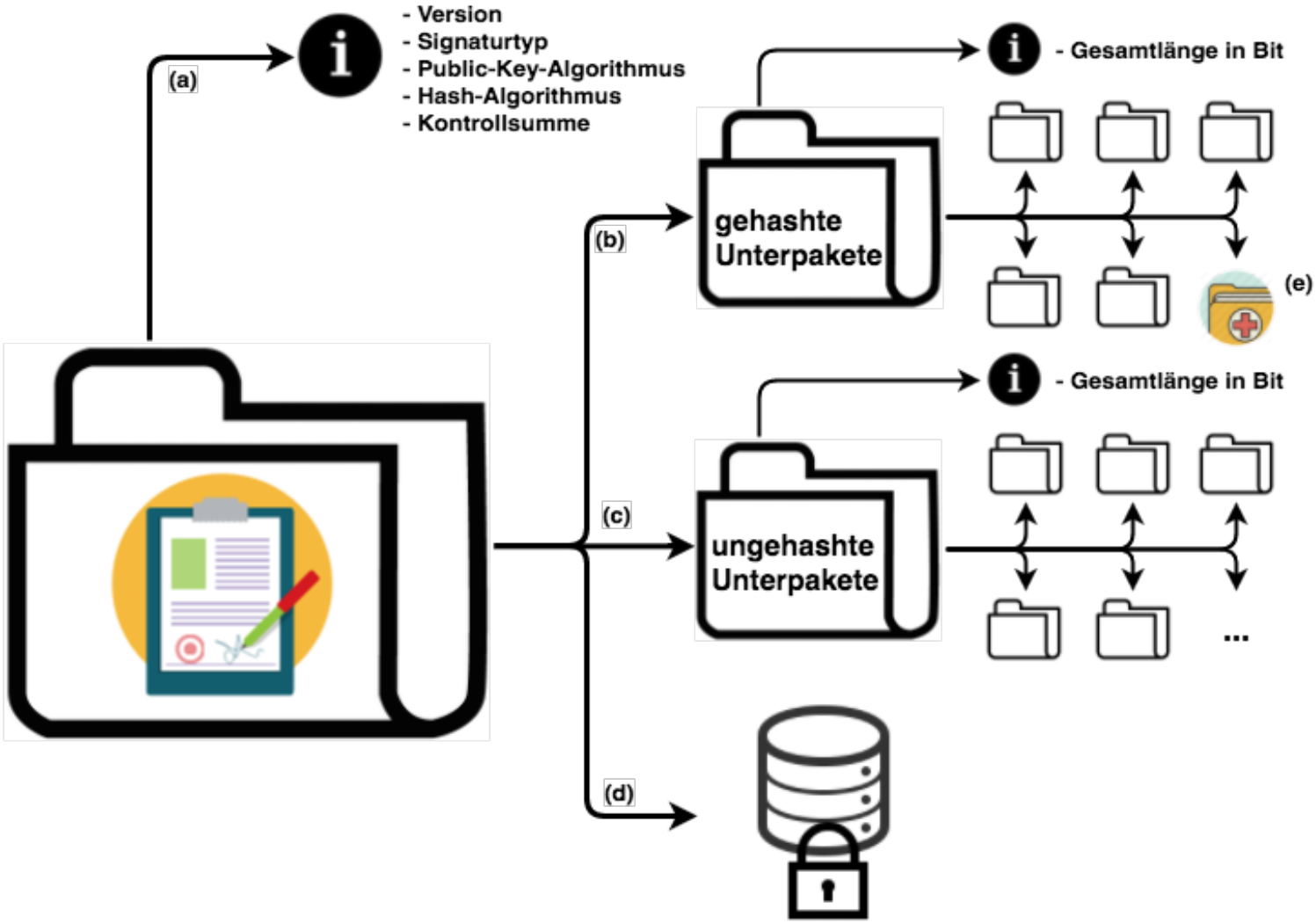
Sometimes: Include it in often used standards.

Blind signature verification in OpenPGP

Make it flexible

- Allow key reuse.
- Do not change the signature definition.

Blind signature verification in OpenPGP



gpg2 --list-packets

Blind signature subpacket

- hashed
- critical flag
- algorithm id

```
# off=1149 ctb=c2 tag=2 hlen=2 plen=130 new-ctb
:signature packet: algo 19, keyid AF62A13E6E7E4D7F
  version 4, created 1496050152, md5len 0, sigclass 0x11
  digest algo 10, begin of digest 99 02
  hashed subpkt 2 len 4 (sig created 2017-05-29)
  critical hashed subpkt 100 len 1 (blind signature verification algorithm: 1)
  subpkt 16 len 8 (issuer key ID AF62A13E6E7E4D7F)
  data: [254 bits]
  data: [515 bits]
[...]
```

No difference during verification

- gpg2 --import [signature_file]
- gpg2 --check-sigs [Name/Mail]

```
pub   rsa4096/391E99FF 2014-02-23 [SC] [expires: 2018-02-23]
uid          [ unknown] John Doe <b5z2xdpp3p@brfkv.anonbox.net>
sig!3        391E99FF 2014-02-23  John Doe <b5z2xdpp3p@brfkv.anonbox.net>
sig!1        6E7E4D7F 2017-05-29  ecc_nist_p_256
```

Defense against the Dark Arts

Edward Snowden, Guardian, 11 March 2014

- "Crypto works. It's not an arcane black art. It is a basic protection, the Defense Against the Dark Arts for the digital world. We must implement it, actively research it."

Github: 0ndorio

Some source code: `https://github.com/0ndorio/verify_me`