

Signature schemes variations

- Multisignatures: several signers create a signature on a single message, that is shorter and faster to verify than when a standard signature scheme is used in a straightforward way.
- Aggregate signatures: similar to multisignatures, but the signers sign different messages.
- Threshold signatures: a group of n users holds a single public key. Each user holds a share of the secret key. At least t users need to cooperate to produce a valid signature on a message.
- Proxy signatures: a signer delegates its signing capabilities to a proxy.

1

- Group signatures: a group of users holds a single public key. Each user can sign on behalf of the group and remain anonymous, except from the manager of the group, who manages the group (joining and revocations of users).
- Ring signatures: similar to group signatures, but there is no group manager.
- Blind signatures: any user can obtain a signature on a message of its choice from a signer, such that the signer does not know what it signed.
-

2

Signcryption

- It is often desirable to achieve both privacy and authenticity in the public key setting.
- Signcryption is a public key primitive that assures privacy and authenticity of transmitted data
- Signcryption must be considered in the two-user or multi-user setting.

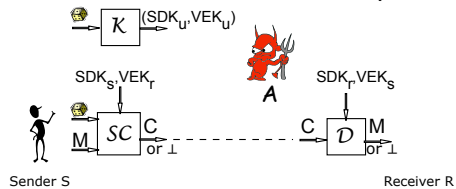


3

Signcryption

A scheme AS is specified a key generation algorithm \mathcal{K} , a signcryption algorithm SC , and a designcryption algorithm \mathcal{DSC} .

$$AS = (\mathcal{K}, SC, \mathcal{DSC})$$



It is required that for every $M \in \text{MsgSp}$ and every $(SDK_S, VEK_S), (SDK_R, VEK_R)$ that can be output by \mathcal{K} , $\mathcal{DSC}((SDK_R, VEK_S), SC((SDK_S, VEK_S), M)) = M$

4

Security of signcryption

- A signcryption scheme is not simply an asymmetric encryption scheme.
- Strong security notions in terms of privacy (IND-CCA) and authenticity (INT-CTXT) can be defined somewhat similarly to those for authenticated encryption.
- However, as we cannot only consider the single-user setting anymore, we may consider
 - outsider and insider security, depending on whether an adversary is an outsider (given only the public keys), or an insider (knows the secret key of a sender or a receiver)
 - two-user and multi-user security (the latter needs to consider a possibility of "identity fraud")
- As before an interesting question is how to properly compose an asymmetric encryption scheme and a digital signature scheme in order to get a secure signcryption

5

Some results

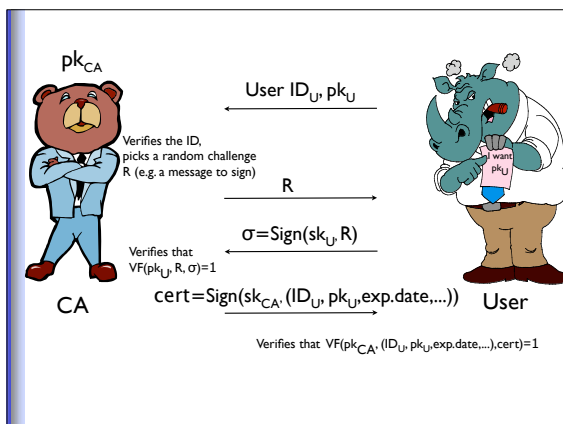
- If an encryption scheme is IND-CPA secure and a signature scheme is SUF-CMA secure then Encrypt-then-Sign signcryption scheme (defined naturally) is IND-CCA and INT-CTXT secure in the outsider two-user model.
- To insure security in the multi-user model one needs to
 - whenever encrypting something, add the public key of the sender to a message to encrypt
 - whenever signing something, add the public key of the receiver to a message to sign

6

Public Key Infrastructure (PKI)

- Asymmetric cryptography assumes that
 - public keys are public
 - public keys are authentic and tied to users' identities
 - users' secret keys have not been compromised
- PKI's goal is to support this setting
- To make the PKI work we need to trust someone (e.g. a "trusted third party" - a Certification Authority (CA))

7



8

- The PKI also
 - makes the certified public keys, the corresponding identities and the certificates public
 - maintains the public certificate revocation list (CRL)
- The PKI may be hierarchical with CAs certifying other CAs.
- X.509 is the standard for digital certificates developed by the International Telecommunications Union (ITU).

9

Secret key sharing

- Security of all symmetric and asymmetric schemes relies on secrecy of a secret key.
- How to make a secret key "more secret"?
- An idea: let's split a secret key K and store the shares in different places (e.g. on n different computers), such that
 - any t shares allow to reconstruct K
 - if $t-1$ computers become compromised, we are still fine in that no one can learn anything about K from $t-1$ shares
- To do any harm an adversary must compromise t computers
- This is (t,n) -secret sharing scheme.

10

Shamir's secret sharing

- Let p be a large prime.
- To (t,n) share a secret $z \in \mathbb{Z}_p$:
 - Choose $t-1$ random elements of \mathbb{Z}_p : a_1, \dots, a_{t-1} . Let $a_0 = z$.
View these as the coefficients of a polynomial f of degree $t-1$, meaning $f(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1}$
 - Store $y_i = f(i)$ on each computer $i = 1, \dots, n$.

- To recover the secret given t pairs (i, y_i) for $i \in S$ use the Lagrange interpolation to find:

$$z = a_0 = f(0) = \sum_{i \in S} y_i \prod_{j \in S, j \neq i} \frac{-j}{i-j}$$

- The scheme is unconditionally secure

Can be pre-computed













11

- There are several weaknesses of the Shamir's secret sharing protocol:
 - if some parties cheat during the secret reconstruction, the secret cannot be recovered and others cannot detect cheating
 - the dealer needs to be trusted
- A verifiable secret sharing protocol allows to overcome these difficulties
- It is also desirable that parties be able to perform secret-key operations (decryption or signing) such that no party holds the whole secret key at any time
- Threshold schemes allow to achieve this

12

(2,2) Visual secret sharing

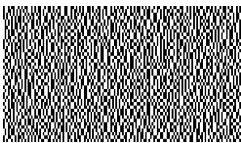
- Let's consider a protocol to (2,2)- share a black-and-white image:
 - for each pixel compute the shares as follows:

| pixel | | share #1 | share #2 | superposition of the two shares |
|-------|----------|---|---|---|
| □ | $p = .5$ |  |  |  |
| | $p = .5$ |  |  |  |
| ■ | $p = .5$ |  |  |  |
| | $p = .5$ |  |  |  |

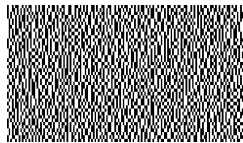
13

An example

Share 1



Share 2



The result? See in class

14

References

- Signcryption
 - Y. Dodis, "Signcryption. Short Survey." Available from <http://theory.lcs.mit.edu/~yevgen/academic.html>
 - J. H. An, Y. Dodis and T. Rabin, "On the Security of Joint Signature and Encryption," Eurocrypt 2002. Available from <http://theory.lcs.mit.edu/~yevgen/academic.html>
 - J. H. An, "Authenticated Encryption in the Public-Key Setting: Security Notions and Analyses." Available from <http://eprint.iacr.org/2001/079>
- PKI
 - Internet X.509 Public Key Infrastructure - Certificate Management Protocol (CMP). Internet draft. Available from <http://www.ietf.org/internet-drafts/draft-ietf-pkix-rfc2510bis-09.txt>
 - C. Ellison and B. Schneier, "Ten risks of PKI." Available at <http://www.schneier.com/paper-pki.html>

15

References

- Secret Sharing
 - David Wagner's lecture notes. Available from <http://www.cs.berkeley.edu/~daw/teaching/cs276-s04/22.pdf>
- Visual cryptography
 - Doug Stinson's visual cryptography page. <http://www.cacr.math.uwaterloo.ca/~dstinson/visual.html>

16