



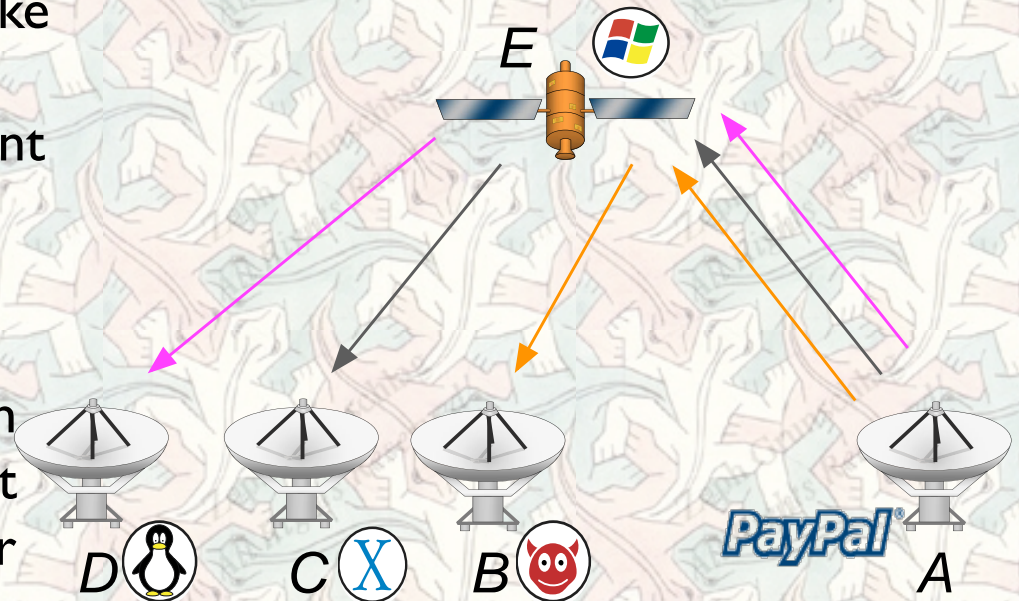
Digital Signatures

Prof. Zeph Grunschlag

(Public Key) Digital Signatures

PROBLEM: Alice would like to prove to Bob, Carla, David, ... that has really sent them a claimed message.

GOAL: Alice signs each message so individuals can verify authenticity without pre-agreed secret keys for MAC's and no interatction



Notions of Security

Note: Security *not* built-in to above. Haven't even defined conditions for V rejecting by returning 0.

Chosen message attack: with non-negligible probability, Eve is able to create a valid message-signature pair after studying other message-signature pairs of her choice where the signatures were obtained by querying a signing oracle.

Digital Signatures

DEF: A **digital signature scheme** consists of a tuple (M, K, G, S, V) where

- M - message space
- K - key space with each key $= (pk, sk)$
- G - PPT key generator picks key k of security parameter $l : k \xleftarrow{R} G(1^l)$
- S - PPT algorithm for signature $S_{sk}(m)$ from secret key and message. Write:
- V - verifier which is a Las-Vegas PPT decider s.t. $V_{pk}(m, S_{sk}(m)) = 1$ if (pk, sk) is a valid key.

Security Definition

DEF: An **existential adaptive message forger** is an adversarial algorithm A that has access to a signing oracle O_S and outputs a valid message-signature pair (m, s) for some message m_{new} that was not a query to O_S .

DEF: A signature scheme (M, K, G, S, V) is *existentially unforgeable under adaptive chosen message attack* if every PPT forger A succeeds in forging with following negligible probability:

$$\Pr[V_{sk}(A^{O_S}(pk)) = 1]$$

Note: “**chosen** message attack” doesn’t mean Eve can choose which message to forge at the end. Only that she can choose which message to forge during cryptanalysis.

Other Notions

Attack goals (just saw *existential forgery*)

- selective forgery - attacker can forge some messages of choice (non-negligibly)
- universal forgery - can forge any message
- total break - attacker can recover sk

Attack methods (saw *adaptive chosen message*)

- chosen message attack - attacker chooses fixed set of messages to have signed before cryptanalysis
- known message attack - when given random message-signature pairs, attacker succeeds with non-negligible probability
- key only attack - attacker only has pk

Naïve RSA Signature

- $K = (p, q, e)$ with p, q primes of equal size, e relatively prime to $(p-1)(q-1)$. Set $n = p \cdot q$
- $pk = (n, e)$, $sk = (n, d)$ with $d = e^{-1} \bmod p$
[same key-pair as RSA encryption]
- Alice signs m with $S_{sk}(m) = x^d \bmod n$
- Bob verifies m by applying $V_{pk}(m) = x^e \bmod n$

Same arguments as with RSA encryption show that key security is equivalent to factoring n .

Naïve Rabin Signature

Same idea as with RSA. Sign by “decrypting”
verify by “encrypting”. Need to restrict
message to $QR(n)$ so that square roots
exists. Other numbers are *un-signable*.

- Alice signs messages in $QR(n)$ by sending a square root of message m
- Bob verifies by squaring signature and checking that result equals message.

Similar argument as for Rabin encryption shows:

existential forgery with known messages
 \Leftrightarrow extracting square roots \Leftrightarrow factoring n

Naïve El-Gamal

- Dlog based signature scheme, similar to commercial Digital Signature Standard (DSS)
- $sk = (\text{prime } p, \text{primitive } \alpha, \text{exponent } x)$
- $pk = (p, \alpha, \beta = \alpha^x \text{ mod } p)$
- Signing: let m denote the message. Signer chooses random index k rel. prime to $p-1$

$$S_{sk}(m) = [a, b] = [\alpha^k, k^{-1}(m - \alpha^k x) \text{ mod } (p - 1)]$$

- Verifying: Notice that

$$a^b = \alpha^{k^{-1}(m - \alpha^k x)} \equiv_p (\alpha^k)^{k^{-1}(m - \alpha^k x)} \equiv_p \frac{\alpha^m}{(\alpha^x)^{\alpha^k}} \equiv_p \frac{\alpha^m}{\beta^a}$$

In particular, to verify by ensuring that

$$\alpha^{-m} \beta^a \equiv_p a^b$$

El-Gamal Motivation

- If we can solve Dlog, would be able to find the exponent x , thus finding the secret key and unabashedly signing any message we want to.
- Intuitively, for arbitrary message m , that's the only way to do it. Complete mastery of forgery expected to allow producing two distinct verifiable triples (m, a, b) & (m', a', b') satisfying $a^b = (a')^{b'} \Rightarrow \alpha^{-m} \beta^a \equiv_p \alpha^{-m'} \beta^{a'}$ which by previous techniques solves Dlog problem.
- Unknown if El-Gamal break implies Dlog alg.

Naïve Rabin Break

Similar argument as for Rabin encryption's cracking under chosen ciphertext attack shows:

Rabin is totally broken under chosen message attack.

Naïve RSA Break

As defined, existentially forgeable under chosen signature attack

- Choose any desired signature, s .
- Use public key (n,e) and let $m = s^e \bmod n$
- (m, s) are valid message-signature pair by definition, but had no control over m .
- Practical patch to this problem is to sign hash of m , not m itself.

Naïve El-Gamal Break

Existentially forgeable as follows: Choose any number w that is relatively prime to $p-1$.

Choose any number z at all. Let $a = \alpha^z \beta^w$,
 $b = -aw^{-1} \bmod (p-1)$, $m = -azw^{-1} \bmod (p-1)$

Notice that $a^b = (\alpha^z \beta^w)^{-aw^{-1}} = \frac{\alpha^{-azw^{-1}}}{\beta^a} = \frac{\alpha^m}{\beta^a}$

which shows that (m, a, b) is valid according to El-Gamal.

Hashing before signing fixes this issue.

Cramer-Shoup Stateless DSA

Provably secure digital signature algorithm if...

- collision resistant hash function exist for security parameter l s.t. $h : \{0, 1\}^* \rightarrow \{0, 1\}^l$
- strong RSA conjecture: negl. probability of extracting *any* non-trivial root of random number mod $p \cdot q$ is (prod. of k -bit primes)
- Sophie Germain conjecture: **non-negl.** prob. that random number is a **Sophie Germain prime** (p and $2p+1$ both prime)

Cramer-Shoup Keys

For hash-security parameter l (size of hash function outputs) and security parameter k :

- SK : secret keys are factors (p,q) with $(p-1)/2$ and $(q-1)/2$ equal k -bit Sophie Germain primes.
- PK : public keys consist of the product $n=p \cdot q$, random quadratic residues g and x , and a random $l+1$ -bit prime \tilde{e} . Summary:

$$pk = (n, g, x, \tilde{e})$$

Cramer-Shoup Signature

For message m , $S(m) = (e, y, \tilde{y})$ defined by:

- e : random $l+1$ bit prime
- \tilde{y} : random quadratic residue mod n
- y : defined by:
 - $\tilde{x} = \tilde{y}^e \cdot g^{-h(m)} \pmod{n}$
 - $y = (x \cdot g^{h(\tilde{x})})^{e^{-1} \pmod{\phi(n)}} \pmod{n}$

Cramer-Shoup Verify

1. Check that e is an odd number not divisible by \tilde{e}
2. Compute $\tilde{x} = \tilde{y}^{\tilde{e}} \cdot g^{-h(m)} \pmod{n}$
3. Check that $x \equiv_n y^e \cdot g^{-h(\tilde{x})}$

Cramer-Shoup Security

THM: Supposing the existence of h , the strong RSA assumption and the non-negligible proportionality of Sophie Germain primes, the Cramer-Shoup signature scheme is existentially secure against adaptively chosen message attack.