Public Key Cryptography
PKC ‘ 2000

18-20 january 2000 - Melbourne - Australia

Design Validations for Discrete Logarithm Based Signature Schemes

Ernest Brickell
David Pointcheval
Serge Vaudenay
Moti Yung

Overview

- Introduction
- DL-based standards
- Trusted El Gamal Types Signature Schemes
- Security Properties
- Some Applications
- Conclusion

Introduction

Signature Scheme = Authentication

Key-Gen: outputs a pair of secret-public keys

Sign: on input a message and the secret key, outputs a signature *Sig*

Ver: on input a message, a signature and a public key, checks whether the signature has been produced, on this message, using the secret key related to the public one

Security Notions

(existential) unforgeability

(under adaptively chosen-message attacks):

no adversary, who has access to a signature oracle, can produce a new pair message-signature but with negligible probability

Previous Results

Random Oracle Model:

some objects are seen *ideal*

e.g. hash function = ideal random function

- RSA-based:

FDH-RSA, PSS (Bellare-Rogaway EC '96)

- DL-based:

Schnorr (JoC '91 - Pointcheval-Stern EC '96)

DL-based Signatures

El Gamal (1985)

p large prime and $g \in \mathbf{Z}_p^*$ of large order

Key-Gen: $X \in \mathbf{Z}_{p-1}$ and $Y = g^X \bmod p$

secret key: X and public key: Y

Sign(M): $k \in \mathbf{Z}_{p-1}^*$ and $R = g^k \bmod p$

then $S = (M - XR) / k \bmod p\text{-}1$

$\rightarrow \sigma = (R, S)$

Ver(M,σ): check whether $Y^R R^S = g^M \bmod p$

Security

- El Gamal (1985): existential forgery
- Schnorr (1989): many improvements
  - in a prime subgroup (efficiency)
  - message hashed together with r

$\Rightarrow$ unforgeability (Random Oracle Model [PS96])

- DSA (1994) and KCDSA (1998):

  message hashed alone: unforgeability?

  Standards $\neq$ Provably Secure Schemes!

  $\Rightarrow$ many attacks (e.g. ISO 9796-1)

DL-based Signatures

p and q large primes such that $q \mid p$-1

and $g \in \mathbb{Z}_p^*$ of order q

Key-Gen: $X \in \mathbb{Z}_q$ and $Y = g^X \bmod p$

- secret key: X
- public key: Y

Sign(M): $k \in \mathbb{Z}_q^*$ and $R = g^k \bmod p$

and …

DL-based Standards

- Digital Signature Algorithm (DSA)

Sign(M): (k, R), $T = R \bmod q$ and $U = H(M)$
then $S = (U+XT)/k \bmod q$ $\rightarrow \sigma = (T, S)$

Ver(M,σ): with $U=H(M)$, $T \stackrel{?}{=} \left(g^{\frac{U}{S}} Y^{\frac{T}{S}} \bmod p \right) \bmod q$

- Korean Certificate-based Digital Signature Algorithm (KCDSA)

Sign(M): (k, R), $T = G(M)$ and $U = H(R)$
then $S = (k - T \oplus U)/X \bmod q$ $\rightarrow \sigma = (U, S)$

Ver(M,σ): with $T=G(M)$, $U \stackrel{?}{=} H\left(g^{T \oplus U} Y^{S} \bmod p\right)$

DSA-Variants

DSA(M): $k \in \mathbf{Z}_q^*$ and $R = g^k \bmod p$,
$T = R \bmod q$ and $U = H(M)$
then $S = (U+XT)/k \bmod q$ $\rightarrow \sigma = (T, S)$

DSA-I(M): $T = G(R)$ and $U = H(M)$

$$T \stackrel{?}{=} G\left(g^{\frac{U}{S}} Y^{\frac{T}{S}} \bmod p \right) \text{ where } U = H(M)$$

DSA-II(M): $T = G(R)$ and $U = H(M,T)$

$$T \stackrel{?}{=} G\left(g^{\frac{U}{S}} Y^{\frac{T}{S}} \bmod p \right) \text{ where } U = H(M,T)$$

Security

DSA $\rightarrow$ DSA-I: $x \rightarrow x \bmod q$ replaced by G

DSA-I: provably unforgeable
if both G and H are random oracles

But "$x \rightarrow x \bmod q$" $\neq$ random oracle!

$\Rightarrow$ no consequences for DSA

KCDSA: provably unforgeable
if both G and H are random oracles

Can we weaken the assumptions:
Two Random Oracles?

Hash Functions

Classical properties for Hash Functions:

- random oracle: ideal random function
- l-collision-freeness:
  there do not exist l pairwise distinct elements $(x_1, \dots, x_l)$ such that
  $$h(x_1) = \dots = h(x_l)$$
- l-collision-resistance:
  it is computationally impossible to find l pairwise distinct elements $(x_1, \dots, x_l)$ such that
  $$h(x_1) = \dots = h(x_l)$$

Trusted El Gamal Type Signature Schemes

- p and q large primes such that $q \mid p\text{-}1$ and $g \in \mathbf{Z}_p^*$ of order q
- G and H two hash functions:
  G: $\{0,1\}^* \rightarrow \mathbf{G}$ and H: $\{0,1\}^* \rightarrow \mathbf{H}$
  such that $q/2 < |\mathbf{G}|,|\mathbf{H}| < q$
  - G is seen as a random oracle
  - H has just practical properties

Key-Gen: $X \in \mathbf{Z}_q$ and $Y = g^X \bmod p$

Sign(M): $k \in \mathbf{Z}_q^*$ and $R = g^k \bmod p$

TEGTSS Characteristics

- Three Functions:
  - F_1: $\mathbf{Z}_q \times \mathbf{Z}_q \times \mathbf{G} \times \mathbf{H} \rightarrow \mathbf{Z}_q$
  - F_2: $\mathbf{Z}_q \times \mathbf{G} \times \mathbf{H} \rightarrow \mathbf{Z}_q$
  - F_3: $\mathbf{Z}_q \times \mathbf{G} \times \mathbf{H} \rightarrow \mathbf{Z}_q$

such that, for all $(a,b,T,U) \in \mathbf{Z}_q \times \mathbf{Z}_q \times \mathbf{G} \times \mathbf{H}$

$$F_2(F_1(a,b,T,U),T,U) + b\, F_3(F_1(a,b,T,U),T,U) = a \bmod q$$

- TEGTSS Verification Equation:
  a tuple (W,S,T,U) is said “valid” if
  $W = g^{E_g} Y^{E_Y} \bmod p$
  where $E_G = F_2(S,T,U)$ and $E_Y = F_3(S,T,U)$

TEGTSS - I

Sign(M): (k, R), $T = G(M)$ and $U = H(R)$
then $S = F_1(k,X,T,U)$ $\rightarrow \sigma = (S,T,U)$

Ver(M,σ): check if $T = G(M)$ and $U = H(W)$,
where $W = g^{E_G} Y^{E_Y} \bmod p$
with $E_G = F_2(S,T,U)$ and $E_Y = F_3(S,T,U)$

Properties: for two tuples (W_i,S_i,T_i,U_i), $i=1,2$

- $T_1 \neq T_2 \Rightarrow F_3(S_1,T_1,U_1) \neq F_3(S_2,T_2,U_2)$
- (W_1,S_1,T_1,U_1) fixed, $U_2 \rightarrow T_2$ one-to-one map such that $F_3(S_1,T_1,U_1) = F_3(S_2,T_2,U_2)$

TEGTSS - I: Security

KCDSA: $F_1(k,X,T,U) = (k - T \oplus U)/X \bmod q$
$F_2(S,T,U) = T \oplus U \bmod q$
and $F_3(S,T,U) = S \bmod q$

Security Claim:

If H is a random oracle
but G is just collision-resistant then
existential forgery = extraction of X

Proof:

use of the Forking Lemma [PS96]

TEGTSS - II

Sign(M): (k, R), $T = G(R)$ and $U = H(M,T)$
then $S = F_1(k,X,T,U)$ $\rightarrow \sigma = (S,T,U)$

Ver(M,σ): check if $T = G(W)$ and $U = H(M,T)$,
where $W = g^{E_G} Y^{E_Y} \bmod p$
with $E_G = F_2(S,T,U)$ and $E_Y = F_3(S,T,U)$

Properties: for given (T, E_G, E_Y), there exists a unique pair (U,S) such that

$$E_G = F_2(S,T,U) \text{ and } E_Y = F_3(S,T,U)$$

TEGTSS - II: Security

DSA-II: $F_1(k,X,T,U) = (U + XT)/k \bmod q$
$F_2(S,T,U) = U/S \bmod q$
and $F_3(S,T,U) = T/S \bmod q$

Security Claim:

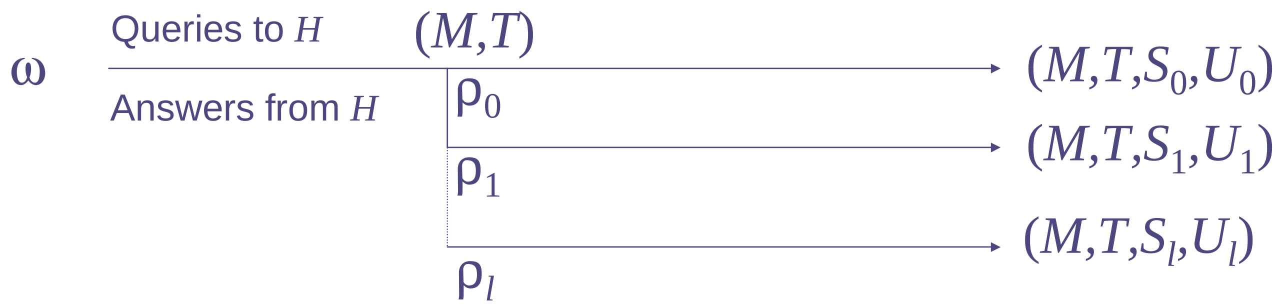
If H is a random oracle, but

- $x \rightarrow G(x)$ is $(l + 1)$-collision-resistant
- **<u>OR</u>** $x \rightarrow G(g^x \bmod p)$ is $(l + 1)$-collision-free

then existential forgery = extraction of X

Improved Forking Lemma

Existential forgery: Probability of success = ε



(M,T,S_0,U_0) valid after $1/\varepsilon$ attempts: prob. > 1/3

Good "beginning" (before $H(M,T)$): prob. > 1/8

Other valid output after $24Q\log(2l)/\varepsilon$ attempts: prob. > 1/3

$\Rightarrow$ $l+1$ valid outputs, same (M,T): prob. > 1/72

but distinct $l+1$ oracle answers: prob. > 1/96

Proof

Using the Improved Forking Lemma, after less than $25lQ\log(2l)/\varepsilon$ executions of the adversary,

$\rightarrow M, T, (S_0,U_0), (S_1,U_1), \ldots, (S_l,U_l)$ such that

$W_i = g^{E_{Gi}}\, Y^{E_{Yi}} = g^{t_i} \bmod p$

with $E_{Gi} = F_2(S_i,T,U_i)$, $E_{Yi} = F_3(S_i,T,U_i)$ and $t_i = E_{Gi} + X\, E_{Yi}$

Then $T = G(g^{t_i} \bmod p)$ for every i

with pairwise distinct E_{yi}

- G $l+1$-CR: $\exists i \neq j\ W_i = W_j$ then X
- $G(g^x)$ $l+1$-CF: $\exists i \neq j\ t_i = t_j$ then X

Applications: KCDSA

KCDSA:

- provably unforgeable
  if both G and H are random oracles
- provably unforgeable
  if H is a random oracle
  but G just collision-resistant

Applications: DSA-II

DSA-II:

- provably unforgeable
  if both G and H are random oracles
- provably unforgeable
  if H is a random oracle but
  - $R \rightarrow G(R)$ just multi-collision-resistant
  - or $x \rightarrow G(g^x)$ just multi-collision-free

Applications: DSA

DSA-II:

- for any random G, $x \rightarrow G(g^x \bmod p)$ is likely $(\log q)$-collision-free

DSA:

- a collision for

$$x \rightarrow (g^x \bmod p) \bmod q$$

would lead to an important weakness in the original DSA

Consequences

TEGTSS-II: unforgeability if

- H is a random oracle
- $x \rightarrow G(x)$ is $(l+1)$-collision-resistant

- a random function $G: \{0,1\}^* \rightarrow \{0,1\}^{80}$ is 5-collision-resistant
- a signature is a pair $(S,T) \in \mathbf{Z}_q \times \mathbf{G}$ $\Rightarrow$ only 200 bit-long

Conclusion

Many standards have been broken (e.g. ISO 9796-1) whereas efficient provably secure schemes exist.

- DSA, why?
  Whereas many slight variants would have been provably secure?
- KCDSA is provably secure
  (even with **only one** random oracle)