Public Key Cryptography
PKC ‘ 2000
18-20 january 2000 - Melbourne - Australia

The Composite Discrete Logarithm and Secure Authentication

David Pointcheval
Département d ’Informatique
ENS - CNRS

David.Pointcheval@ens.fr http://www.di.ens.fr/~pointche

Overview

- Introduction
- Zero-Knowledge vs. Witness-Hiding
- The Discrete Logarithm Problem
- The GPS Identification Scheme
- The New Schemes
- Conclusion

Introduction

Authentication Protocols:

- Identification (Zero-Knowledge Proofs)
- Signatures (Non-Interactive Proofs)
- Blind Signatures (Anonymity)

Previous Work

- Fiat-Shamir (SQRT), Ong-Schnorr (2^k-th roots) Guillou-Quisquater (RSA), Schnorr (DL(p))
  - *e*-th roots and discrete logarithm

  $\Rightarrow$ high computational load
- PKP, SD, CLE, PPP
  - combinatorial problems

  $\Rightarrow$ high communication load

Tools: ZK vs. WI

- Zero-Knowledge:

(GMR 85)

no information leaked about the secret

- Witness Hiding/Indistinguishability:

(FS 90)

no useful information leaked
about the witness (secret key)

Zero Knowledge

- Advantages:
  - no information leaked about the secret
    $\Rightarrow$ perfect proof of knowledge
    (perfect authentication)
  - non-interactive version
    $\Rightarrow$ signature schemes (FS86 - PS96)
- Drawbacks:
  - simulation $\Rightarrow$ many iterations
  - large computations/communications

One of the best: Schnorr's protocols

Witness Indistinguishability

- Advantages:
  - no **useful** information leaked
    about the witness (secret)
    $\Rightarrow$ the good property for authentication
  - non-interactive version
    $\Rightarrow$ signature schemes
  - no simulation $\Rightarrow$ only **one** iteration
  - large computations/communications?

Candidates: Okamoto schemes (Crypto '92)
but less efficient than Schnorr's

The Discrete Logarithm Problem

- Setting:
  - n and m large numbers such that $m|\varphi(n)$
  - g in $\mathbb{Z}_n^*$ of order m
- Secret: x in $\mathbb{Z}_m^*$
- Public: $y=g^x \bmod n$
- Usually DL(p):

  $n=p$ and $m=q \mid p$-1
  are both large prime integers

The Composite Discrete Logarithm

- Composite Modulus: DL(n)
  - n hard to factor (e.g. $n=pq$)
  - DL(n) harder than FACT(n) and DL(p) where p is the greatest prime factor of n

$\Rightarrow$ DL(n) combines the two strongest problems

- Factorization: FACT(n)

$$g^x = g^y \bmod n \Rightarrow \gcd(g^{x-y} \bmod n, n) \neq 1$$

New Setting: α-strong modulus

- **α-strong prime** p: $p=2r+1$
  and for any $m \leq \alpha$, $\gcd(m,r)=1$
- **α-strong RSA modulus** n: $n=pq$
  and both p and q are α-strong primes
- **asymmetric basis** $g \in \mathbf{Z}_n^*$:
  2 divides $\mathrm{Ord}_p(g)$ but not $\mathrm{Ord}_q(g)$

Theorem: a collision of $x \rightarrow g^x \bmod n$ provides the factorization of n

The Schnorr 's Identification

- Common Data:
  - p and q large primes such that $q \mid p$-1
  - g in $\mathbf{Z}_p{}^*$ of order q
- Keys: s in $\mathbf{Z}_q$ and $v=g^{-s} \bmod p$

$$r \in \mathbf{Z}_q \text{ and } x = g^r \bmod p \quad \xrightarrow{x}$$

$$\xleftarrow{e} \quad e \in \mathbf{Z}_{2^k}$$

$$y = r + es \bmod q \quad \xrightarrow{y}$$

$$x \stackrel{?}{=} g^y v^e \bmod p$$

The Schnorr 's Identification

$$r \in \mathbf{Z}_q \text{ and } x = g^r \bmod p \quad \xrightarrow{x}$$

$$\xleftarrow{e} \quad e \in \mathbf{Z}_{2^k}$$

$$y = r + es \bmod q \quad \xrightarrow{y} \quad x \stackrel{?}{=} g^y v^e \bmod p$$

- Efficiency:
  - (r, $x=g^r$) precomputed
  - just $r+es \bmod q$ to do on-line

Could we do better?

The GPS Scheme

Girault (EC '91) - Poupard-Stern (EC '98)

- $n=pq$ large RSA modulus
- g in $\mathbf{Z}_n{}^*$ of large order (unknown)
- Keys: s in $\mathbf{Z}_S$
  and $v=g^{-s} \bmod n$

> k - security level
> $\log S$ - size of the secret
> $\log R$ - size of the random

$$
\begin{array}{lcl}
r \in \mathbf{Z}_R \text{ and } x = g^r \bmod n & \xrightarrow{x} & \\
 & \xleftarrow{e} & e \in \mathbf{Z}_{2^k} \\
y = r + es & \xrightarrow{y} & x \stackrel{?}{=} g^y v^e \bmod n
\end{array}
$$

The GPS Scheme

$$
\begin{array}{lcl}
r \in \mathbf{Z}_R \text{ and } x = g^r \bmod n & \xrightarrow{x} & \\
 & \xleftarrow{e} & e \in \mathbf{Z}_{2^k} \\
y = r + es & \xrightarrow{y} & x \stackrel{?}{=} g^y v^e \bmod n
\end{array}
$$

- Poupard-Stern:
  - no adversary can succeed but with negligible probability over g and e. Otherwise she can break DL(n)
  - it is statistically zero-knowledge

if $S > \mathrm{Ord}(g)$ and $S.2^k/R$ negligible

The GPS Scheme

- Advantages:
  - high security level: DL(n)
  - just $r+es$ to do on-line
    no more modular reduction
- Drawbacks:
  - zero-knowledge: several iterations
  - $S > \mathrm{Ord}(g)$ (for any g): $S > \lambda(n)$
    and $R >> S.2^k$

    $\Rightarrow$ large parameters (S and R)
    and large secret key (s)

New Scheme (New Setting)

- $n=pq$ large 2^k-strong RSA modulus
- g asymmetric basis in $\mathbf{Z}_n^*$ of large order
- Keys: s in $\mathbf{Z}_S$
  and $v=g^{-s} \bmod n$

- k - security level
- $\log S$ - size of the secret
- $\log R$ - size of the random

$$r \in \mathbf{Z}_R \text{ and } x = g^r \bmod n \quad \xrightarrow{x}$$

$$\xleftarrow{e} \quad e \in \mathbf{Z}_{2^k}$$

$$y = r + es \quad \xrightarrow{y} \quad x \stackrel{?}{=} g^y v^e \bmod n$$

Properties

$r \in \mathbf{Z}_R$ and $x = g^r \bmod n$	$\xrightarrow{x}$	
	$\xleftarrow{e}$	$e \in \mathbf{Z}_{2^k}$
$y = r + es$	$\xrightarrow{y}$	$x \stackrel{?}{=} g^y v^e \bmod n$

- Statement: this protocol is
  - a proof of knowledge of s (= $-\log_g v$) relative to FACT(n)
  - statistically witness-indistinguishable

  if $S > \mathrm{Ord}(g)$ and $S.2^k/R$ negligible

Efficiency

- Drawbacks:
  - lower security level: FACT(n)
    but isn't that enough…?
- Advantages:
  - **still** just $r+es$ to do on-line (no modular reduction)
  - witness-indistinguishable:
    $\Rightarrow$ **only one** iteration with large k
  - **still** $S > \mathrm{Ord}(g)$ and $R >> S.2^k$
    but $\mathrm{Ord}(g)$ can be small (160 bits)
    $\Rightarrow$ **small secret key and numbers**

More Concrete Efficiency

- Practical sizes:
  - security parameter: k=24
  - n a 1024-bit 2^k-strong RSA modulus
  - g of 160-bit long order
  - the secret key s is less than $S=2^{168}$
  - information leakage: $2^{k'} = R/2^k.S = 2^{64}$
- Computations:
  - Mult(24,168) and Add(256,192)
- Communications:
  - only 360 bits (45 bytes)

Signature

- Data:
  - $n=pq$ large 2^k-strong RSA modulus
  - g asymmetric basis in $\mathbf{Z}_n^*$ of large order
  - Keys: s in $\mathbf{Z}_S$ and $v=g^{-s} \bmod n$
- Signature:
  - $r\in \mathbf{Z}_R$ and $x = g^r \bmod n$
  - $e = \mathrm{H}(m,x)$
  - $y = r + es$

  $\rightarrow$ signature of $m = (e,y)$
- Verification:

$$e = \mathrm{H}(m, g^y v^e \bmod n)$$

Security Properties

Statement:

if $S > \mathrm{Ord}(g)$, then

- an existential forgery
- under an adaptively chosen-message attack
- in the random oracle model

is harder than factorization

Blind Signature

- $n=pq$ large 2^k-strong RSA modulus
- g asymmetric basis in $\mathbf{Z}_n{}^*$ of large order
- Keys: s in $\mathbf{Z}_S$ and $v=g^{-s} \bmod n$

$r \in \mathbf{Z}_R$ and $x = g^r \bmod n \xrightarrow{x}$

$\beta \in \mathbf{Z}_M$

$h = g^{\beta} \bmod n$

$$\boxed{\begin{array}{l} \gamma \in \left\{-2^k,\ldots,2^k\right\} \\ \alpha = xhv^{\gamma} \bmod n \\ \varepsilon = \mathrm{H}(m,\alpha) \\ e = \varepsilon - \gamma \quad \text{until } e \in \mathbf{Z}_{2^k} \end{array}}$$

$\xleftarrow{e}$

$y = r + es \xrightarrow{y}$

$x \stackrel{?}{=} g^y v^e \bmod n$

Security Properties

Properties: this protocol is

- a statistically blind signature
  if R/M is negligible
- statistically witness-indistinguishable
  if $S > \mathrm{Ord}(g)$
  and $S.2^k/R$ is negligible
  (two witnesses $\rightarrow$ factorization of n)

$\Rightarrow$ a "one-more" forgery

- under a parallel attack
- in the random oracle model

is harder than the factorization of n

Parameters

Scheme	GPS	New ID	New Sign.
Modulus	$\|n=pq\|$=1024 bits with $\|p\|=\|q\|$=512		
Ord(g)	1022 bits	160 bits	
Security (k)	24	24	128
Information leakage (k')	64		
S R	1030 bits 1118 bits	168 bits 256 bits	168 bits 360 bits
Size	1222 bits	360 bits	488 bits
Security	= DL(n)	>Fact(n)	>Fact(n)

Conclusion

- New setting for GPS schemes:
  - very efficient identification (precomputation)
  - very efficient signature (“on the fly”)
  - very small secret key (less than 200 bits)
  - security relative to factorization (at least)
    (and then security of Schnorr’s schemes)
- New blind signature scheme
  - very efficient for the signer
  - with security relative to factorization