GPS

or how to sign on the fly with low-cost smart cards

IEEE P1363 meeting, Miami, 9-10 January 2003
Marc Girault, France Telecom
Guillaume Poupard, DCSSI
Jacques Stern, Ens Ulm
GPS – basic motivation

- Provably secure on the fly public key authentication with a low-cost smart card and a contactless interface

- Not possible with RSA (even if using a cryptoprocessor) nor with most public key algorithms
Applications

- Contactless, wireless transactions
- Mobile telephones
- Electronic purse, electronic payment
- Teleticketing
- Toll systems
- Transport (passengers, goods)
History of GPS

- **EC ’91**: Girault, *Self-Certified Public Keys*
- **EC ’98**: Poupard and Stern, *Security Analysis of a Practical « on the fly » Authentication and Signature Generation*
- **2000**: project « *Turbo-signatures* » (french Ministry of Research) : France Telecom, ENS, Bull CP8, Cryptogram
- **2003**: - selection by IST NESSIE project (?);
  - submission to ISO (and Journal of Cryptology)
What is GPS?

- GPS is a zero-knowledge proof of knowledge of a discrete logarithm which works in any group, with direct applications to public key authentication and digital signatures.
- Very flexible, many possible trade-offs between security and efficiency.
GPS (basic) authentication scheme

**Parameters**: $n = p \cdot q$ an RSA modulus
$g$ an integer of large order modulo $n$

**Secret key**: $s \in \mathbb{S}$

**Public key**: $v = g^{-s} \mod n$

---

**Prover**

$r < A$
$x = g^r \mod n$

**Verifier**

$y = r + c \cdot s$

$y \cdot v^c \equiv x \mod n$

(Size checking steps are omitted)
GPS basic scheme – two remarks

- The underlying problem is « short exponent composite discrete logarithm »

- \( n \) may be a « system » parameter (i.e. common to all system users) or part of user’s public key
  - if \( n \) is a system parameter, it should be very large (e.g. 2048 bits)
  - if \( n \) is part of the public key, it should be reasonably large (e.g. 1024 bits) and Chinese Remainder Technique can be used
Security analysis: conclusions

- Probability of impersonation = $1/B$

- Statistically zero-knowledge if $A$ is much larger than $B \times S$ ($y = r + c \cdot s$)
GPS in practice: the coupons

- Commitment $x = g^r \mod n$ can be precomputed (e.g. by the smart card, when it is idle)

- Commitments can be hashed (FiSh)
  - C ’94: GiSt ($|H| = 88$ bits)
  - Cardis 2000: Gi ($|H| = 50$ bits)

- The prover stores
  - the $r$ values or a seed for a pseudo-random generator that generates them
  - coupons $H(g^r \mod n)$
Performances of GPS (1)

In C (GMP), using a standard PC (1,2 GHz)

- Parameter sizes: $|n|=1024$, $|S|=160$, $|B|=35$
  - computation of a coupon $x = 4$ ms
  - computation of the response $y = 0$ ms
  - verification = 5 ms
Performances of GPS (2)

On a low-cost smart card
(8-bit CPU, RAM = 100 bytes, program = 300 bytes)

- Parameter sizes: $|n|=1024$, $|S|=160$, $|B|=35$
  - up to 655 coupons in 4 Kbytes of EEPROM
  - computation of the response $y$ (10 MHz) < 1 ms
    (< 10 ms if $|S|=1024$)
  - communications (19200 bits/s) = 45 bytes (19 ms)
Various options

- Can be easily turned into a signature scheme
- Other groups can be used
- Verification can be server-aided
- If $S=n$, at least as secure as RSA
- Keys can be made identical with RSA keys
Signature scheme

- Just replace the challenge $c$ by the pseudo-challenge $H(x,m)$, $H$ a collision-free hash-function and $m$ the message (FiSh heuristic)
- $c$ is larger but on-line computation is still very fast
- Secure in the random oracle model (PoSt 98)
Using other groups

- GPS is generic: it can be used in any (finite) group where discrete logarithms are hard, not only $\mathbb{Z}_n^*$

- e.g.: $\mathbb{Z}_p^*$ ($p$ prime → Schnorr on the fly), elliptic curves, class groups of imaginary quadratic orders,…
Server-aided verification

- To speed-up verification [GiQu 02]:
  - let \( g = f^e(\mod n) \) (typically \( e = 65537 \))
  - ask a (powerful, untrusted) server to compute \( Y = f^y(\mod n) \)
  - check that \( Y^e v^c = x (\mod n) \)

- Security is now related to the intractability of extracting \( e \)-th roots modulo \( n \)
RSA security as a minimum (1)

- By choosing a full-size secret \((S=n)\), the underlying problem is composite discrete logarithm, harder than factorization (hence harder than RSA)

- The secret \(s\) can be chosen
  - randomly in the interval \([0, n[\)
  - equal to a specific value, in order to optimize some features (see following slide)
RSA security as a minimum (2)

- Specific choices of $n$, $g$ and $s$ allow to reduce the public key to $n$, hence GPS to be compatible with many RSA key management primitives (in particular it can be embedded in a RSA PKI)

- For example:
  - $g=2$ and $s = n – \phi(n)$ (s is « half-size ») \[PoSt 00\]
  - $g=2$, $e$ small prime and $es = 1 \pmod{\phi(n)}$ (the key pair is identical with a RSA key pair) \[GiPa 02\]
Why to choose (or not) GPS signature scheme rather than...? (1)

- ...factorization-based schemes (RSA, E-Sign, GQ,...)
  - (much) faster on-line computation
  - based on a harder assumption*
  - still usable if factorization is no longer intractable
  - but verification / overall computation is (much) slower

- ...discrete-log-based schemes (DSA, Schnorr,...)
  - faster on-line computation
  - RSA-compatible (security, key management)*
  - verification can be efficiently server-aided
  - but signatures are larger

* if \( n \) is full-size

IEEE P1363 meeting, Miami, 9-10 January 2003
Why to choose (or not) GPS rather than...? (2)

- «new problems»-based schemes (NSS, SFLASH,...)
  - faster on-line computation
  - relies on « old problems » (well-established security)
  - but verification / overall computation is much slower
Using GPS as a cryptographic tool

- GPS is widely used in complex primitives, such as bounded range commitment, group signatures, short proofs of knowledge of factoring...(but reference to GPS is generally omitted)

- Applications to electronic cash, verifiable secret sharing, verifiable public keys, fair encryption of private keys,...
Copyright situation

➢ IPR statement:

“In case GPS is finally selected as a NESSIE Primitive, France Télécom and La Poste declare that they are willing to grant non-exclusive, non transferable, worldwide licences [...] on fair, reasonable and non discriminatory terms and conditions [...] to any third party which [...] shall submit an equivalent undertaking[...]”.
Conclusion

- A flexible scheme, which combines well-established security and efficiency; more precisely:
- Allows to meet very strong time requirements in secure transactions, while possibly remaining RSA-compatible (in terms of security and key management)
- Embedding in current infrastructures and standards is under study