CERIAS

The Center for Education and Research in Information Assurance and Security

On the Security of Short Schnorr Signatures

Jeremiah M Blocki Seunghoon Lee
Department of Computer Science, Purdue University

Motivation / Contribution

- Schnorr Signatures: $4k$-bits long (short) with k-bit security
  - ✓ One hash value ($2k$-bits) + One group element ($2k$-bits)
  - ✓ BLS Signatures are shorter ($2k$-bits), but less practical
- Folklore: $3k$-bit signatures with shorter hash function (k-bits)
  - ✓ No security proof
- Our Result: Folklore is right!
  - ✓ Concrete security proof in Generic Group Model + Random Oracle Model shows
  - ✓ $3k$-bit signatures with k-bits of security

Generic Group Model

- For a cyclic group $G = \langle g \rangle$ of order q, elements of G are encoded by bit strings of length ℓ in a cryptographic scheme. Let $\mathbb{G}$ be a set of bit strings of length ℓ, then
$$\tau : G \to \mathbb{G}$$
gives the natural representation of G in $\mathbb{G}$.
- The key idea is that an adversary attacks a primitive is only given access to a randomly chosen encoding of a group instead of efficient encodings.
- On input $(a,b) \in \mathbb{G}\times\mathbb{G}$, the $\mathrm{Mult}(\cdot,\cdot), \mathrm{Inv}(\cdot)$ and $\mathrm{Pow}(\cdot,\cdot)$ oracles return
$$\mathrm{Mult}(a,b) = \tau\left(\tau^{-1}(a)\cdot\tau^{-1}(b)\right)$$
$$\mathrm{Inv}(a) = \tau\left(\left(\tau^{-1}(a)\right)^{-1}\right)$$
$$\mathrm{Pow}(a,b) = \tau\left(\left(\tau^{-1}(a)\right)^{b}\right)$$
if $a, b \in \tau(G)$.

k-bits of Security

- We say that a scheme yields "k-bits of security" if any attacker running in time at most t should forge a signature with probability at most $t/2^k$ and this should hold for all $t \le 2^k$.

Open Questions

- Could one achieve the same concrete security bound for ECDSA/DSA in the generic group and random oracle model?
- Are we able to identify any concrete statements that have been proved about BLS signatures in the generic group and random oracle model?

The Schnorr Signature Scheme[1]

Kg:
$sk \xleftarrow{\$} \mathbb{Z}_q\,;\, pk \leftarrow \tau(g^{sk})$
Return (pk, sk)

Sign(sk, m):
$r \xleftarrow{\$} \mathbb{Z}_q\,;\, I \leftarrow \tau(g^r)$
$e \leftarrow \mathsf{H}(I\|m)$ (first k-bits)
$s \leftarrow r + sk\cdot e \bmod q$
Return $\sigma = (s, e)$

Vfy(pk, m, σ):
$I \leftarrow \mathrm{Mult}(\mathrm{Pow}(\tau(g), s), \mathrm{Pow}(\mathrm{Inv}(pk), e))$ $= \tau(g^s \cdot g^{-sk\cdot e})$
If $\mathsf{H}(I\|m) = e$
Then return 1
Else return 0.

Figure 1. The Schnorr Signature Scheme

- Our Analysis: H is a random oracle that outputs k bits (can truncate output if needed)
- Typical: Hashes are $2k$ bits long ($4k$-bit signatures)

Our Results

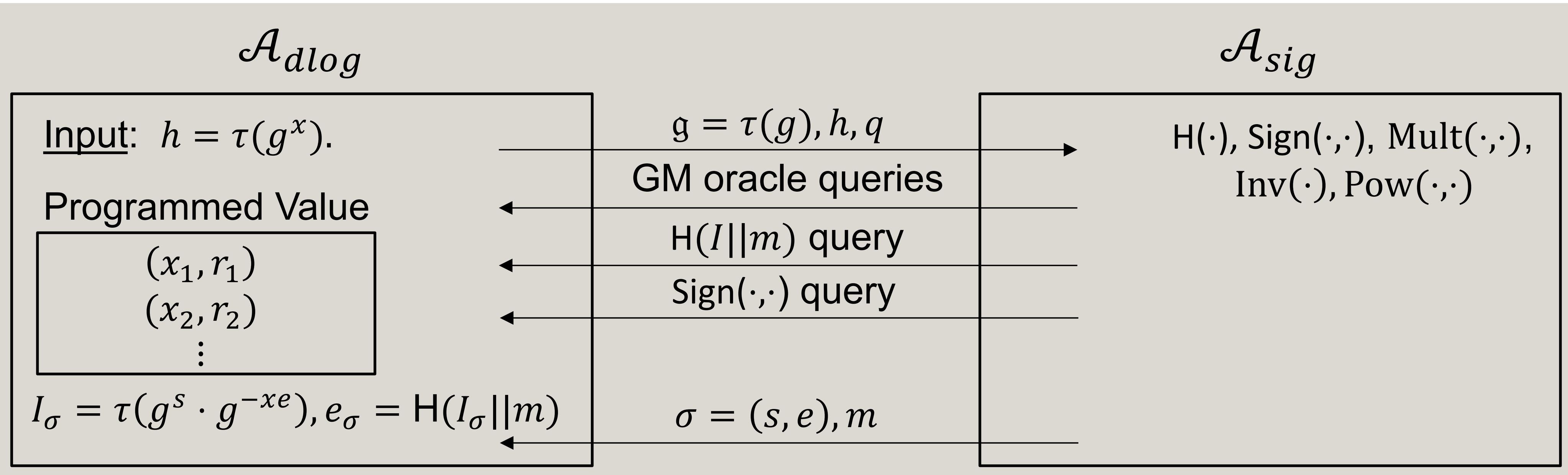
- We have the following (informal) form of theorem which guarantees a $3k$-bit signature with k-bits of security:

Theorem. Let $\mathcal{A}$ be an adversary attacking Schnorr signature scheme running in time at most t. Then the probability that the adversary successfully forge a signature is bounded by
$$\mathrm{Adv}(\mathcal{A}) \le O\left(\sqrt{\frac{t}{q}} + \frac{t}{2^k} + \frac{t^2}{q}\right)$$
under the Generic Group Model of order q and Random Oracle Model.

- Set $q = 2^{2k}$ and select a hash function H with k output bits. The resulting signatures have k-bits of security and length $k + \log_2 q = k + 2k = 3k$.

Security Reduction

- Security reduction starts with the attacker $\mathcal{A}_{sig}$ that attacks the modified Schnorr signature and builds the discrete-log attacker $\mathcal{A}_{dlog}$.



Sign(m) without having x
Pick s, e randomly
Compute $\tau(g^s), \tau(\tau^{-1}(h)^e) = \tau(g^{xe})$
Compute $I = \tau(g^s \cdot g^{-xe})$
If $\mathsf{H}(I\|m)$ previously queried, then
Return $\bot$
Define $e \coloneqq \mathsf{H}(I\|m)$
Return $\sigma = (s, e)$

$\mathrm{Mult}(\tau(g), \tau(g)) = \tau(g^2) \Longrightarrow$ "Known"
$\mathrm{Mult}(\tau(g^2), h) = \tau(g^{2+x}) \Longrightarrow$ "Partially Known"
Neither in both sets $\Longrightarrow$ "Unknown"

Case 1: Query $\mathsf{H}(I\|m)$ not made before
Case 2: I_σ in "Unknown"
Case 3: I_σ in "Partially Known"

Figure 2. A Security Reduction

References

1. Schnorr (1989). Efficient Identification and Signatures for Smart Cards. *CRYPTO '89*.
2. Neven, G., Smart, N. & Warinschi, B. (2009). Hash function requirements for Schnorr signatures. *Journal of Mathematical Cryptology*, 3(1), pp. 69-87.
3. Seurin Y. (2012). On the Exact Security of Schnorr-Type Signatures in the Random Oracle Model. *EUROCRYPT 2012*.
4. Boneh, D., Lynn, B., & Shacham, H. (2004). Short Signatures from the Weil Pairing. *Journal of Cryptology*. 17 (4): 297-319.

PURDUE UNIVERSITY Discovery Park

CERIAS