On the Multi-User Security of Short Schnorr Signatures with Preprocessing

Jeremiah Blocki Seunghoon Lee
Department of Computer Science, Purdue University

Summary

- Schnorr Signatures: $4k$ bits long with k bits of security
- *Short* Schnorr Signatures: $3k$ bits long (truncating hash output)

Questions.
- k bits of multi-user security for *short* Schnorr signatures?
- Is the *short* Schnorr signatures secure against preprocessing attacks?

Our Result.
- Single/Multi-user security of short Schnorr signatures (in GGM+ROM)
- Multi-User Security of short Schnorr signatures against preprocessing
- Applicable to other Fiat-Shamir-based signatures

Schnorr Signature Scheme [2]

$\mathsf{Kg}(1^k)$:
$\mathsf{sk} \xleftarrow{\$} \mathbb{Z}_p$
$\mathsf{pk} \leftarrow g^{\mathsf{sk}}$
return $(\mathsf{pk}, \mathsf{sk})$

$\mathsf{Sign}(\mathsf{sk}, m)$:
$r \xleftarrow{\$} \mathbb{Z}_p$; $I \leftarrow g^r$
$e \leftarrow \mathsf{H}(I \| m)$
$s \leftarrow r + \mathsf{sk} \cdot e \mod p$
return $\sigma = (s, e)$

$2k$ bits $2k$ bits

$\mathsf{Vfy}(\mathsf{pk}, m, \sigma)$:
Parse $\sigma = (s, e)$; Compute $R \leftarrow g^s \cdot \mathsf{pk}^{-e}$
if $\mathsf{H}(R \| m) = e$ **then**
return 1
else return 0

Short: truncate it to k bits!

k Bits of Multi-User Security

- If any attacker is given N public keys $\mathsf{pk}_1, \ldots, \mathsf{pk}_N$, one can forge a signature σ that is valid for *any one* of these public keys with probability $\leq t/2^k$, where t is the attacker's running time

Generic Group Model (GGM) [3]

- Any elements of a cyclic group $G = \langle g \rangle$ of order p can be encoded by binary strings of length ℓ, with encoding function $\tau : G \to \mathbb{G}$ (set of ℓ-bit strings)
- **Key Idea:** an adversary is only given access to a randomly chosen encoding of group elements
- On input $(\mathfrak{a}, \mathfrak{b}) \in \mathbb{G} \times \mathbb{G}$ and $n \in \mathbb{Z}_p$,

$$\mathtt{Mult}(\mathfrak{a}, \mathfrak{b}) = \tau\left(\tau^{-1}(\mathfrak{a}) + \tau^{-1}(\mathfrak{b})\right),$$
$$\mathtt{Inv}(\mathfrak{a}) = \tau\left(\left(\tau^{-1}(\mathfrak{a})\right)^{-1}\right),$$
$$\mathtt{Pow}(\mathfrak{a}, n) = \tau\left(\left(\tau^{-1}(\mathfrak{a})\right)^{n}\right),$$

if $\mathfrak{a}, \mathfrak{b} \in \tau(G)$.

Our Results in Detail

Multi-User Security of Short Schnorr Signatures

Theorem (informal).
Given N public keys, any attacker making at most q queries can forge a short Schnorr signature with probability $\mathcal{O}((q+N)/2^k)$ in the GGM (of order $p \approx 2^{2k}$) plus ROM.

- If $k = 112$ (i.e., $p \approx 2^{224}$) and $N = 2^{32}$ (more than the half of the entire world population), an attacker making at most $q = 2^{80}$ queries succeeds with probability $\leq \varepsilon \approx 2^{-32}$
- A naïve reduction loses a factor of N, i.e., $\varepsilon' \approx N\varepsilon \approx 1$!

Multi-User Security of Short Schnorr Signatures against Preprocessing

Theorem (informal).
Given N public keys, any *preprocessing* attacker making $\leq q_{\text{pre}}$ queries and outputs an S-bit hint (preprocessing phase) and making $\leq q_{\text{on}}$ queries (online phase) can forge a *key-prefixed short* Schnorr signature with probability $\widetilde{\mathcal{O}}\left(\frac{SN(q_{\text{on}}+N)^2}{p} + \frac{q_{\text{on}}}{2^k} + \frac{Nq_{\text{pre}}q_{\text{on}}}{p^2}\right)$ in the GGM (of order $p > 2^{2k}$) plus ROM.

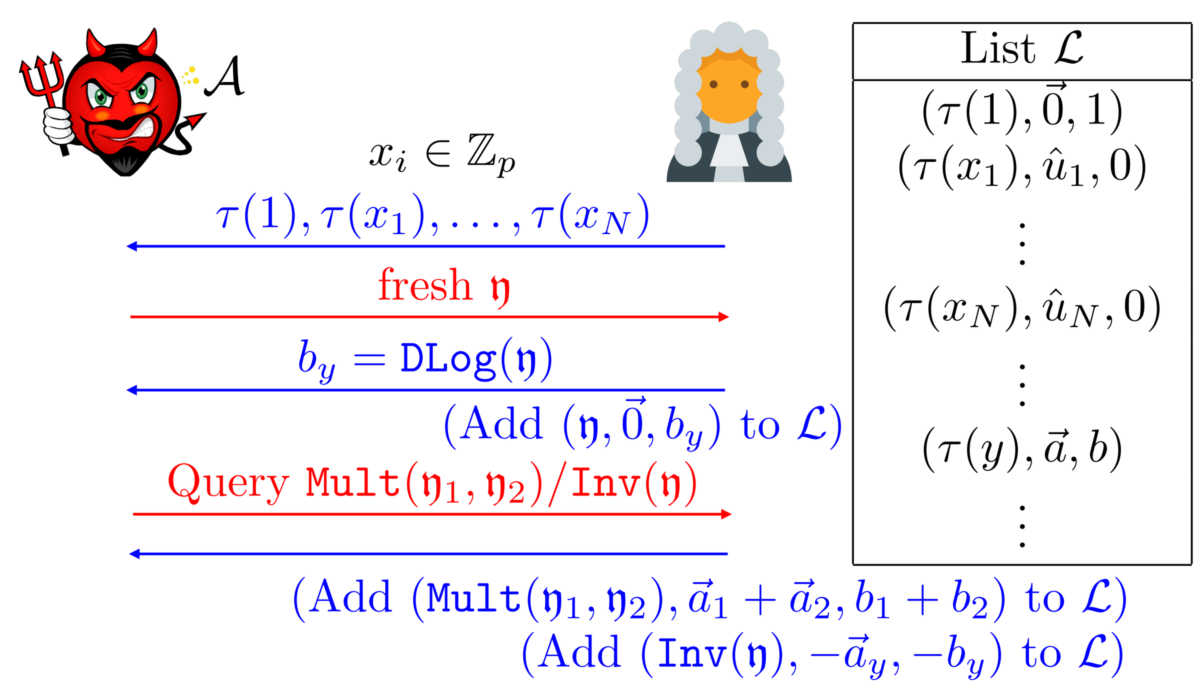
- Why key-prefixing? ► Not to disallow $e = 0$ signatures!
- Setting $p \approx 2^{2k}SN$ and $S = 2^{k/2}$ and $N = 2^{k/4}$, signature length: $k + \log_2 p \approx 3.75k$
- Still achieving k bits of multi-user security!

Similar bounds are applicable to other Fiat-Shamir-based signatures, i.e., key-prefixed Chaum-Pedersen-FDH signatures [5] and *short* Katz-Wang signatures [6]

- Katz-Wang signature length: $4k$ bits
- Our *short* Katz-Wang signature length: $3k + \log_2 N + \log_2 S + \log_2(2k + \log_2 NS)$ bits (for preprocessing)

Our Techniques

The Multi-User Bridge-Finding Game

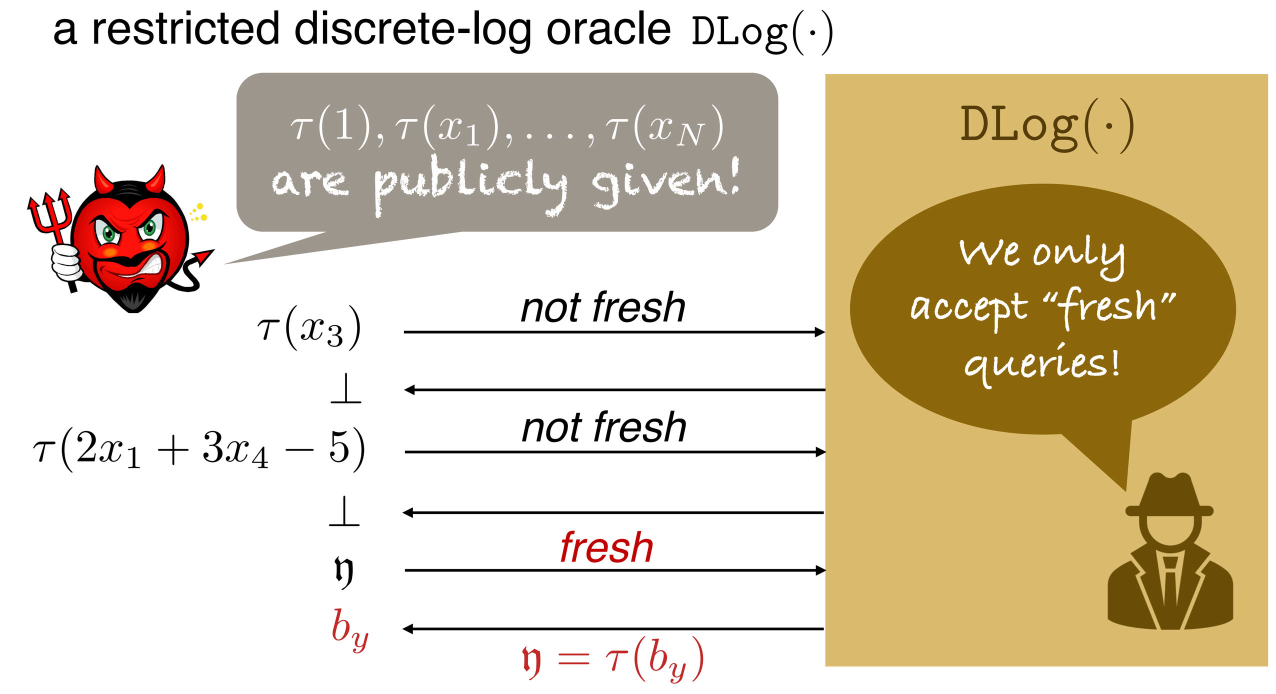


- The attacker's goal: find a *non-trivial linear relationship* between $x_1, \ldots, x_N$ after making queries to the generic group oracles
- $\mathcal{A}$ is even given access to $\mathtt{DLog}(\cdot)$ for "fresh" queries
- A preprocessing attacker can win the game with probability $\mathcal{O}(SNq^2 \log p/p)$
  ✓ The proof adapts a compression argument [4]

Corollary. The 1-out-of-N discrete-log problem is hard even for a preprocessing attacker!

Restricted Discrete-Log Oracle

- We consider a *stronger attacker* who is given access to a restricted discrete-log oracle $\mathtt{DLog}(\cdot)$

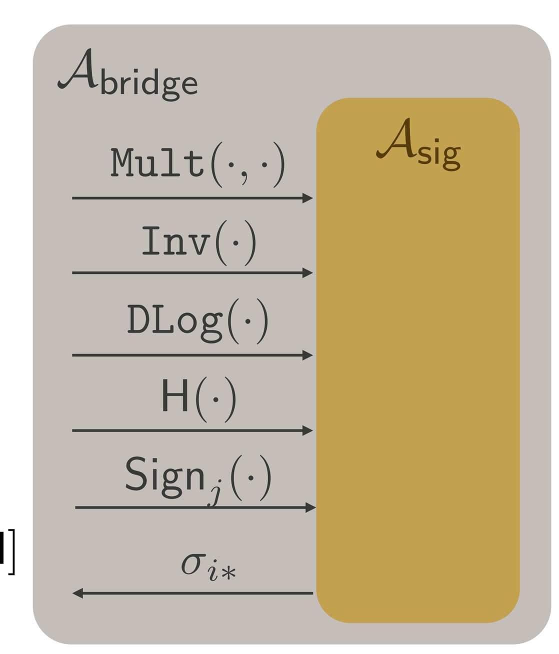


- Why restricted? ► To rule out trivial attacks!

Security Reduction

- Bridge inputs $\tau(x_1), \ldots, \tau(x_N)$ are public signing keys when simulating $\mathcal{A}_{\text{sig}}$
- The reduction also make use of a programmable random oracle whenever $\mathcal{A}_{\text{sig}}$ queries $\mathsf{Sign}_j(\cdot)$ for a particular user $j \in [N]$
- Probability of failure events is negligible:

$\Pr[\mathcal{A}_{\text{sig}} ☺] \leq \Pr[\mathcal{A}_{\text{bridge}} ☺] + \Pr[\mathsf{Fail}]$
$\leq \mathcal{O}\left((q+N)/2^k\right)$



Reduction in the Preprocessing Setting

- A *time-bounded* ($\leq 2^{3k}$) preprocessing attacker
- Random oracle compression argument
  (if prob. of bad event too large ► can compress RO!)

References

1. Jeremiah Blocki and Seunghoon Lee. On the Multi-User Security of Short Schnorr Signatures with Preprocessing. *EUROCRYPT 2022.*
2. Claus-Peter Schnorr. Efficient Identification and Signatures for Smart Cards. *CRYPTO '89*, Springer, Heidelberg.
3. Victor Shoup. Lower Bounds for Discrete Logarithms and Related Problems. *EUROCRYPT '97*, Springer, Heidelberg.
4. Henry Corrigan-Gibbs and Dmitry Kogan. The Discrete-Logarithm Problem with Preprocessing. *EUROCRYPT 2018.*
5. David Chaum and Torben P. Pedersen. Wallet Databases with Observers. *CRYPTO '92*, Springer, Heidelberg.
6. Jonathan Katz and Nan Wang. Efficiency Improvements for Signature Schemes with Tight Security Reductions. *CCS '03.*