з: $return\ (pk, sk)$	$3 \colon s \leftarrow r + sk \cdot e \mod p$	3: return 1
$2 \colon pk \leftarrow g^{sk}$	$e \leftarrow H(pk I m)$	2: if $H(pk R m)=e$
1: $sk \leftarrow \mathbb{Z}_p$	1 : $r \overset{\$}{\leftarrow} \mathbb{Z}_p$; $I \leftarrow g^r$	1: $R \leftarrow g^s \cdot pk^{-e}$
$Kg(1^k)$	Sign(sk,m)	$Vfy(pk, m, \sigma)$

Answer 2: Yes, key-prefixed short Schnorr signatures are secure!



Summary of Our Results

Research Questions



Are short Schnorr signatures secure against preprocessing attacks?

Caveats:

 Preprocessing attacker is time-bounded (large enough for practical attacks) Complex proof technique: compression argument

Not a standardized implementation

On the Multi-Cor Security of Short Schoor Signatures with Proprocessing 43

recorded in \mathcal{L} before a query of the form H(I[m]) is over issued — if I is new then we call $\operatorname{Hag}(I)$ before querying the candom cracks. Now define a rathest $\tilde{\mathcal{L}} \subset \mathcal{L}$ as the set of tuples $(L,L) \in G \times \mathbb{R}_+^p \times \mathbb{R}_+$ such that I has exactly zero nonzero densent. See we call a random cracke query $x = (I[m] \times \mathbb{H}_+^p \times \mathbb{H}_+^p) = -2$ whose the tuple $(I,d,k) \in \tilde{\mathcal{L}}$ has already been recorded and the reconser-densent of I in $\tilde{\mathcal{L}}$ (Second like if there were two recorded tuples (I,d,k) and (I,d,d) then are algorithm would have already found a $\operatorname{BEOCE}^{\mathbb{R}^n}$ instance). Thus, the probability onto individual query I is "last" in all most I" and we can see union bounds to upper bound the probability onto individual query I. "last" I is at most I" and I" on a case which bounds to upper bound the probability of I individual query I is "last" I in I and I" and I" and I" I is the second to upper bound the probability of any "bad" I" query as I I [I].

Boundary of Theorem 7. Let $p>2^{2k}$ be a prime number and $N\in\mathbb{N}$ be a permeter. Let (A_{2k},A_{2k}) be a pair of prime algorithms with an encoding $\sup r:\mathbb{R}_p\to 0$ such that A_{2k} extends an S-bet that and A_{2k} reads at most $q^n:=q^n(k)$ queries to the primeir group entries. Then

$$\Pr\left[\mathsf{BridgeChal}_{A_{m,m_n}}^{(N)}(k) = 1\right] \leq \widetilde{\mathcal{O}}\left(\frac{S(q_1^m + N)(q_2^m + 2N)}{p}\right),$$

where the randomness is taken ever the selection of t, the random cente of $A_{\rm loc}$ and the random celes used by the challenger in the bridge game (the line tay, $=A_{\rm loc}^{\rm r}(g)$) is obtained independently of the random centes used by the challenger). In particular, if $q_{\rm loc}^{\rm r} \geq 16N(1+2\log p)$ and $S \geq 26\log(k_{\rm loc})$, then

$$\text{Pr}\left[\text{BridgeChal}_{\mathcal{A}_{m,m_1}}^{1,2}(k)=1\right] \leq \frac{14|S(g^m)^2\log p}{p}.$$

Proof of Theorem 7: We below the same idea from [CR18, Theorem 2], which shows the relationship between the size of the hint S and the probability ε that can stin the moliti-user heidge-finding game. Say that κ map τ is pool if $\langle A_{pin}, A_{pin} \rangle$ when the multi-user heidge-finding game with probability at least $\varepsilon/2$ on τ . That is, τ is good if we have

$$\Pr\left[\mathsf{BridgeChal}_{A_{m},\mathsf{str}_{n}}^{r,S}(k) = 1\right] \geq \frac{\varepsilon}{2},$$

where the probability is taken over the selection of $\mathcal{E} = \{x_1, \dots, x_N\} \in \mathbb{Z}_+^n$, the random usins of A_m , and the random usins used by the challenger in the bridge game (the bint $m_r = A_m^m(g)$ is selected independently of the random usins used by the challenger).

Let $T = \{v_1, v_2, \dots\}$ be the set of good labeling maps. Then by a sunded assempting segments $\Gamma(A_m^m)$, Lemma $A(R_m^m)$, and $\Gamma(R_m^m)$ denotes the sumbout assempting represent $\Gamma(A_m^m)$. Lemma $\Gamma(R_m^m)$, and the observe that the number of injective mappings from R_m to G is $|G(I_m^m)| |G(I_m^m)| = I_m^m$, which implies that $|T| \geq \langle \iota_1(I_m^m) | |G(I_m^m)| = I_m^m$.

On the Muhi-Eur Security of Short Sciencer Signatures with Proprocessing 67

Handling Not(n. n.):

(1) If either of q_1 or q_2 is not in the image of $\pi,$ reply \bot and continue to

(b) If either of η₁, or η₂ is not in the image of π, reply ⊥ and continue to the next query.
(f) If either of η₁, or η₂ is not in the table, then time is a βrad query input. For each such argament s ∈ (η₁, η₂), and the pair [Ring(g), s) to the table and write s to the encoding using log(g = I) bits, where I is the number of inhelicit slowestly in the table.
(2) Otherwise, look up the taples (f₁, η₂), f₂, η₃) in the table where f₁ = f₁(X₁,...,X_n) and f₂ = f₁(X₁,...,X_n).
(a) If (f₁ + f₂, Ralix(g₁, η₃)) is already in the table, simply uply with Ralix(g₁, η₃) in the salid, simply uply with Ralix(g₁, η₃) in the seconding and reply with Ralix(g₁, η₃).
(b) If (f₁ + f₂, Ralix(g₁, η₃)) is not in the table, then add Ralix(g₁, η₃) into the encoding experience log(g = I) bits, where I is the number of labels already in the table is alleasy of in the table is a linear polynomial f = f(X₁,...,X_n) such that f is not identical to f₁ + f₂ (g₁, the orderivent for X₁ and the matry, then encoding. Then one the equation f = g₁(X₁,...,X_n) such that f is not identical to f₂ + f₃ (g₁, the derive as equation X₁ = g(X₁,...,X_n,...,X_n). If no one is a linear polynomial g of X₁,...,X_n and a linear polynomial g of X₁,...,X_n and

W g is not in the image of r, reply ⊥ and continue to the next query.
 R g is not in the table, then this is an fresh query input. Add the pair

(Blog(n), n) to the table. () Otherwise, look up the tuple (f, η) in the table where $f = f(X_1, \dots, X_N)$ is a linear polynomial of N indeterminates X_1, \dots, X_N , and compute

—if.
(a) If (−f, Σav(g)) is already in the takin, simply reply with Σav(g).
(b) If (−f, Σav(g)) is not in the table, then add ∑av(g) to the emoding and reply with Σav(g). Write Emply into the exceeding requires log(g) − f) bits, where f is the number of labels already in the last.
(c) If Enrich in the table but its cosmopositing discrete log raths in the table is a linear polynomial f = f/(X₁,...,X_n) such that f is

On the Multi-User Security of Short Schoor Signatures with Proproceeding 55

 $A_{\rm lig}^{\rm max}(g)$ is solveted independently of the random coins used by the particular; if $q_1^{\rm m} \ge 10N(1+2\log p)$ and $S \ge 10\log(3p)$, then

 $\varepsilon = \frac{14S(g_{\overline{\alpha}}^{m})^{2}\log p}{4} + \frac{Ng_{\overline{\alpha}}^{m}g_{\overline{\alpha}}^{m}}{4} + \frac{g_{\overline{\alpha}}^{m}(g_{\overline{\alpha}}^{m} + g_{\overline{\alpha}}^{m})}{4} + \frac{4(g_{\overline{\alpha}}^{m} + 1)}{4} + \frac{N^{2}(S + k_{1})}{4}$

Proof of Theorem 6: Given a generic afversary with propossing $(\mathcal{A}_{m}^{m}, \mathcal{A}_{m}^{m})$ attacking Schouer agenties wherea, we construct the following efficient generic adjust has with proprocessing $(\mathcal{A}_{m,m}^{m}, \mathcal{A}_{m,m}^{m})$ which true to accord in the 1-cut-of. N generic BHDGS N -finding gener Bridge Chif $_{m,m}^{N}$ - $_{m,m}^{m}$ (0, \mathcal{E}).

Algorithm $(A^{pq}_{\text{inter}}, A^{pq}_{\text{inter}})$: The algorithm is given $p, p = r(1), pk_q = r(x_i), 1 \le i \le N$ as input.

 A^m_{map} simply rare A^m_m to presente as β-lik blot streng.
 A^m_{map} initializes the set H_{map} = () which stores the random conde in put/output pain observed during undes proceedings.
 A^m_{map} takes the liket str_n and shiftalizes the list £ = ((r(1), 0, 1), |ps, φ, ψ) for 1 ≤ i ≤ N), and sum A^m_{map} with the bins str_n and a number of screen to the generic group outsides Ω^m_n = (pk, 1), |xr ∈ j, || Enq. j ∈ j, |xr ∈ j| ∈ j ≤ N, and the random conde N(·). We maintain the broadend that every output of a generic group query during the online phase appears in the list \mathcal{L} . We consider the following cases:

(a) Whenever A_{ab}^{m} solution a query or to the nucleon oracle \mathbb{N} . If there is a pair $(\nu,R)\in\mathbb{N}_{ab}$ for some etting $R\in[0,1]^{n}$ then return R.

wherever previously (i.e., is not in the list \mathcal{L} then we query $b = \operatorname{Han}(a)$ and odd (a, \bar{b} , \bar{b}) to \mathcal{L} . (b) Whenever A_{ij}^{c} whenever a query a to the generic group oracle $\operatorname{Ind}(\cdot)$. If a is not in \mathcal{L} then we immediately query $b = \operatorname{Han}(a)$ and $abb(a, \bar{b}, \bar{b})$ to \mathcal{L} . Otherwise, i.e. \bar{b} is a of a.

If the same is ξ does not assume that φ and φ . Then, we query law (a,b,c) of $\mathcal{L}(a) = \mathcal{L}(b)$ is some d and b. Then, we query law (a,b) = (-d-d-B), output the result and add (1/(-d-B-b), -d, -b) to $\mathcal{L}(b)$. Whenever \mathcal{R}_{ij}^{m} refuses a query a,b is taken generic group create $\mathrm{Rel}(b,\zeta)$, b = 1 if the element a (resp. b) is not in \mathcal{L} then $\mathrm{query} b_i = \mathrm{Rel}_{ij}(b)$ (resp. $b_i = \mathrm{Rel}_{ij}(b)$) and add the element (a,b,b_i) (resp. $b_i,b_j \in \mathcal{L}$. Then we arisen $\mathrm{Rel}(a,b_i) = (-d,b_i) + (d-b_i) + ($

44 J. Wield and S. Lee

Lemma 3. For a prime y_i by $\{A_{mi}, A_{mi}\}$ be a pair of generic algorithms for \mathbb{Z}_p an \mathbb{Q} with an examining map $r: \mathbb{Z}_p \to \mathbb{Q}$ such that A_{mi} analysis an S-ball hall this, and A_{mi} makes at most g_{mi} primeric group small queries. Then there exists a generic algorithm A_{mi} that makes at most $g_{mi} + 2N \log_2 r N$, premeric group expected queries, and, for energy $r: \mathbb{Z}_p \to \mathbb{G}$, if $\operatorname{Pt}_{I_{n}, A_{mi}}[\operatorname{BoligeChal}^{A_{mi}}_{A_{mi}, B_{mi}}(S, S) = 1] \geq \varepsilon$, then for energy $S = \{s_1, \dots, s_N\} \in \mathbb{Z}_p^N$, $\operatorname{Pt}_{X_m}[\operatorname{BoligeChal}^{A_{mi}}_{A_{mi}, B_{mi}}(S, S) = 1] \geq \varepsilon$.

then for every $\ell = (r_1, \dots, r_N) \in \mathbb{Z}_p^n$, $P(x_0)$ Beingle-Charge, $m_i(t, r) = 1 \ge \ell$. Proof. Algorithm $A_{m_i}[w_{t-1}, r_{(t-1)}, \dots, r_{(t-1)}]$ convoices the following: Sample a random $(v_{t-1}, \dots, r_{t-1}) \mapsto 4 \frac{\pi^2}{2}$ and computes $\operatorname{Rel}(v_i(x_i), r_{(t-1)})$ if each $i \in [N]$, using at most $\operatorname{BN}(u_i p_i, N_i p_i)$ group operations, since it would mad at most 2 legge group operations to compute (r_{t-1}) even only $r_i(t-1)$ for each $r_i(t-1)$ and we have extra one operation of $\operatorname{Rel}(t-1)$ to compute $\operatorname{Rel}(r_{(t-1)}, r_{(t-1)})$ for each $r_i(t-1)$. - Ban $A_{t-1}(t-1)$, $r_i(r_1, \dots, r_{(t-1)}, r_{t-1})$, which plays a multi-sure bridge-finding general finding $\operatorname{Cond}(r_{t-1}, \dots, r_{t-1})$, $r_{t-1}(t-1)$, which plays a multi-sure bridge-finding general finding $\operatorname{Cond}(r_{t-1}, \dots, r_{t-1})$. When A_{t-1} extracts 1, then algorithm A_{t-1} size outputs 1, and vice versa.

Observe that during the encention of E_{α} we run A_{α} on $(r(y_{\beta}, x_{\gamma})_{\gamma}, r(y_{\beta}, y_{\gamma})_{\gamma}, r(y_{\beta$

Sow we are both to of the room. So we are both to the proof of Thomos 7. Lemma 3 implies that there exists a pair of generic algorithms (A_{m}, A_{m}^{-}) such that for every $r \in T$ and every $x' = (x_1, \dots, x_N) \in \mathbb{Z}_p^N$, A_{m}^{-} making at most $q_n^{r} = q_n^{r} + 2N \log p + N$ generic group easile queries and we have P_{A_m} . $[bidgeChx_{A_{m,m}^{r,N}}^{r,N}, (k, x) = 1] \geq \epsilon/2$. Now from Lemma 7, we can use $(A_{m}, A_{m}^{r,N})$ to compress any mapping $r \in T$ to a binary string of length at most

 $\log\frac{|G|!}{(|G|-p)!}+S+1-\frac{(r/2)p}{6q_k^{pr}(q_k^{pr}+N)(\log p+1)},$

where the encoding wheree works with probability at least 1/2. The incompressibility argument⁴ of De et al. [DTT10] may that this length must be at least $\log |T| - \log 2$. Hence, we have that

 $\log\frac{|G|}{(|G|-p)!}+S+1-\frac{(\varepsilon/2p}{6q_0^{2r}(q_0^{2r}+S)(\log p+1)}\geq \log\frac{|G|}{(|G|-p)!}-\log\frac{4}{\varepsilon},$ * BOTTON. But it ill says that "Suppose there is a randomized encoding procedure for : $[0,1]^n \times [0,1]^r \to [0,1]^n$ and a decoding procedure $\mathsf{Out} : [0,1]^n \times [0,1]^r \to [0,1]^r$ such that Pr_{1-n} . But Pr_{2-n} . But Pr_{2-n} . But Pr_{2-n} is Pr_{2-n} . But Pr_{2-n} . Since Pr_{2-n} . Sin

66 J. Block and S. Lee

not identical to \tilde{f} (i.e., the coefficients for X_i 's are not all the same), then smooth the regiv to this query as a pointer to the table entry $(f,\operatorname{Inv}(q))$ and add this pointer to the encoding. Then use the equation $f=-\tilde{f}$ to derive an equation $X_j=g(X_1,\dots,X_N,X_N)$ for some j and a finear polynomials g of X_1,\dots,X_N encogs for X_0 , and explace X_j by $g(X_1,\dots,X_N,X_N)$ in the ta-bles

Decoding Routine

The decoding routine is given the encoded string and recovers τ as follows

Extract see, from the first S bits of the encoding.
 Extract the image of τ from the next log (⁽ⁿ⁾₁) bits from the encoding.
 Initialize Table (logar/varies) in fir τ j as on empty list.
 Extract (τ) from the encoding and add (1, τ(1)) to table.
 Repost the following d times in total:
 Choose the findlewing d times in total:
 Choose the find N ratings in the intrographical order of the image of τ that are not in Table. Call these strings η, ..., η, w and add the pairs: (Nr. η, η, ..., (Ex. , η, n) to the table, where R. ..., R. densites the indeterminates that seprement the discrete log of η,'s for i = 1, ..., N.

pairs (M₁, q₁),..., (E₁, q₁) to the table, whose M₁..., E₂ denotes the indeterminates that segment the disorter log of q₁ is for i = 1, ..., M_r.

(b) Decode r^{*} ∈ [[q] after reading log E bits from the encoding. (d) Decode σ^{*} ∈ [[q₁] after reading log g₂, bits from the encoding. (d) Exact σ^{*} ∈ [[q₁] after reading log g₂, bits from the encoding. (d) Exact q₁ (sto. q₂, ..., q₃) for σ^{*} queries using the r^{***} random tops allocated for this instance of A_{qq}. I. If A_{qq} makes the query Ra(1ψ₁, q₂). B. If either a₁ or a₂ is in the image of τ, reply j. B. If either a₁ or a₂ is in the image of τ, but not in the table, then add sentiax (β, q₁) and (β_q, q₂) to the table, when i and j are the mandlest integral random random from the table. C. Sacoth for the table and find the pairs ([[, a₁]) and ([j₁, a₂]), and compute the linear polynomial j₁ + j₂. (i) If (j₁ = j₂, w₁) is already in the radde, then ruphy with m and entalizes to the next query. (2) If there is no ranh w in the table, and if this is not the last ([[**]*) query of this convention, then read large −1 j into from the encoding, where i is the sambles of labels in the table, and decode the bits to continue to the next query.

I. Block and S. Lee
 I. Pult a_i, i₁ randomly and compute t_i = π(s_i − s_js_i) = Na1s(s_i, Project_j, -s_j) where s_i = Proj_j, s_j).
 I. H Sijet_j(t_i(s_i), has been previously queried, then return t_i.
 Otherwise, program High_j(t_i(s_i), s_j) = s_i, and stars s_i = (s_i, s_j).
 This amount that a side offers of querying the Sign, seads in the addition of the tuples |n(s_i), d̄, s_j) = (p_i, p_i, s_j), s_j, s_j) and ⟨n(s_i − s_j, s_j, −s_j, s_j, s_j) to d̄, since these unless are compared using the powering group contains Ino. No.2t.
 (a) The steep points in these same string η such that (s_i, d̄, b̄) ∈ L and (s_j, d̄, d̄) ∈ L for (d̄, d̄) ∈ L (d̄) then we can isomodately have a RSIOCE² instance ⟨n(d̄) − ḡ), d̄, d̄, d̄, d̄) ∈ L and (n(d̄) − ḡ), d̄, d̄, d̄, d̄) ∈ L and (n(d̄) − ḡ), d̄, d̄, d̄, d̄) ∈ L and (n(d̄) − ḡ), d̄, d̄, d̄, d̄) ∈ L and (n(d̄) − ḡ).
 A Then, without has of generality, we can assume that each string η occurs at most occur in the lim L̄.
 A Alther A²_ḡ contypts s_i = (s_i, s_i, s_j) = the lim L̄.
 A Compute (n(d̄), s_i, s_j, s_j, s̄) is the lim L̄.
 Compute (n(d̄), s_j, s_j, s_j, s̄) is necesser that (s_i, d̄, s_j) ∈ L̄.
 Compute (n_i = Posij_j, s_i, s_j, s̄) is consect that (s_i, d̄, s_j) ∈ L̄.
 T Finally, compute ξ_i = Na(1s(s_i, s̄), n(-s_i, s_j)) = r(s_i, s_i, s_{s_j}), which consenses that (L̄_i, -r_i, s_i, s_i) ∈ L̄.
 Analysis, We first remark that if the signature is valid then we must have

Analysis. We first remark that if the signature is valid then we must have $e_{ii} = H(E_{ii}|\mathbf{w}_{ii})$ and $\operatorname{Sing}(E_{ii}) = u_{ii} - x_{ii}x_{ii} = \bar{x}\cdot \bar{x} + b$. We first candow the periodality that the attacker will outputs a valid signature largery after when we are random stacle programming to simulate the boost signing condex without the secret lays. We introduce to neal events beautiful of OrentProgramming such that the probability of a valid signature

 $\Pr\left[SqFoqr_{A_{\text{Lin}_{n},n}^{N}\mathcal{S}}(k)=1\right]-\Pr[DetexProgramming]-\Pr[FulletSign],$

where $\Pr[\operatorname{Sigforgr}_{A_{m,n-1}^N}^N(k) = 1]$ denotes the probability that the stracker is

 $\Pr[\mathsf{Faltofign}] \leq \frac{\eta(f')(g''' + g(f'))}{2},$

On the Shibi-User Security of Short Schnerr Signatures with Proprocessing 6

 $S \ge \frac{cp}{6(q_1^m + 2N \log p + N)(q_1^m + 2N \log p + 2N)(\log p + 1)} - \log \frac{\pi}{\epsilon}$

Without has of generality, we may assume that $z \ge 1/p$, since the probability to find a BRDGE* instance is not lower than solving 1-out-of-N discrete log problem (see Corollary 1), which is advanced hower than 1/p when growing then randomly filteres, we have that $\log \frac{\pi}{2} \le \log(3p)$ and we get $6\left(S + \log(kp)\right)(g_0^{\mathsf{ss}} + 2N\log p + N)(g_1^{\mathsf{ss}} + 2N\log p + 2N)(\log p + 1) \geq \epsilon p,$

 $\varepsilon \leq \frac{6}{s}(S + \log(3p))\left(q_1^m + N + 2N\log p\right)(q_1^m + 2N + 2N\log p)(\log p + 1)$

 $= \tilde{\mathcal{O}}\left(\frac{S(q_1^m + N)(q_1^m + 2N)}{p}\right)$ i.e., if the size of the hint is bounded then the probability of winning the 1-out-oft of generic bridge finding game is also bounded correspondingly. In particular, if $g^a \geq 16N(1+2\log p)$ and $S \geq 10\log(3p)$, then we observe that

 $z \le \frac{6}{n}(S + \log(8p))(q_1^m + N + 2N \log p)(q_1^m + 2N + 2N \log p)(\log p + 1)$ $\leq \frac{6}{p}(1.18)(1.1q^m)(1.3q^m)(1.1\log p) \leq \frac{145(q^m)^2\log p}{p},$

where we have $\log p+1 \le 1.5 \log p$ because $p>2^{20}$ implies $\log p>2k$ and $\log p+1 \le (1+1/(2k)) \log p \le 1.5 \log p$.

Remainster of Lemma 3. Let G be the set of binary strings of length ℓ such that $T' \geq p$. for a prime p. Let $T = \{r_1, r_2, \ldots\}$ be a subset of the labeling functions from \mathbb{Z}_+ to G. Let (A_{pm}, A_{m}) be a pair of generic algorithms for \mathbb{Z}_+ on G such that $p \in \text{corps} r \in T$ and every $\theta = \{s_1, \ldots, s_N\} \in \mathbb{Z}_+^n$, A_m entipote on S-bit above string, A_m makes at most q_m oracle parties, and (A_{pm}, A_m) . satisfy $\Pr_{\delta_{i,i}}$ [finitysChaf] $_{\delta_{i+1}}^N(t,\ell) = 1$] $\geq \varepsilon$, where $i v_i = A_{i+1}^{(0)}(\tau(i))$. Then, five exists a randomized eccooling scheme that compresses elements of T to bitterings of length at most

$$\log\frac{|\Omega|}{(|\Omega|-p)!}+S+1-\frac{cp}{6q_{\rm so}(q_{\rm so}+N)(\log p+1)}.$$

and records with probability at least 1/2. Proof of Lemma 2: The proof works happly the same as it from [CK32] except for some modifications. In the proof of [CK32], they halld as encoding and a deciding routine to construct a randomized exceding scheme. The exceding

(ii) If there is no such w in the table, and if this is the bast (q^{***}) query, then we know that we have a bridge instance-bern. Thus, read a log [Table) this pointer from the semanting and search for the entry in the table with that pointer, say (f, n). Solve the question f = f, e, f_p and p is the the first indeterminate S in the equation. Replace every S is the polynomials in the table with the solution of the equation in that table with the exists table.
ii. If A_m makes the query Ine(x).
ii. If Ā is in the image of r, poly ii.
iii. If Ā is in the image of r, poly ii.
iii. If Ā is in the image of r, but not in the table, then add an entry (S_m) in the table and find the pair (f, s), and compute the innear polynomial −f.
(ii) If (−f, m) is decayl in the table, then reply with w and continue to the next query.
(ii) If (−f, m) is east w as much w in the table, and of this is not the last (g^{***}) query of this excention, then mad lug(x − l) him from the smoothing, where l is the number of labels in the table, and doubt the lists to except m. Now apply with w, and add (−f, m) is the lists to except m. So, any give with w, and add (−f, m) to the table and continue to the next query.
(ii) If there is no such w in the table, and if this is the last (q^{***}) query of this excention, then mad lug(x − l) him from the modeling and much for the table and continue to the next query.
(ii) If there is no such w in the table, and if the in the last (q^{***}) query, then we know that we have a bridge innersor here. Thus, read a lug(Table) pointer from the encoding and much for the coupling B −f m on p is the first independent of the table independent on the encoding of the table with the continue the equation so that there is no longer S in the continue table.
iii. Bread the values of all the remaining indetermination as they appear in the table.

The total encoding length will be calculated as follows

- the hint τ (5 bits), - the exceding of the image of τ (log $\binom{m}{p}$ bits),

- the excoting of the image of v (log (^m_k) bits),
- the index s' which demons the successful execution of A_m (sling R bits),
- the serical analysis of total question y' (of log pan bits),
- for the st' entry that is added to the tubble (0 ≤ t < [Tailed), if the entry security as assumption to an indextreminate that has been resolved by finding a BRDGS' instance (at most log [Subble bits),</p>
- a otherwise, log |s - t) bits, and
- the remaining discrete log values, encoded using log |p - t| bits each, where t ∈ (!Tabbe(..., p - 1).

On the Multi-User Security of Short Schnerr Signatures with Proprocessing 52

Claim 4. Pr[DetexProgramming] $\leq \frac{N q_0^{\rm ext} q_1^{\rm ext}}{p!}$.

Casins 4. Py[DetextProgramming] $\leq \frac{Com_{\pi}}{2} \mathbb{E}_{\pi}$.

We pass the proof of Claim 8 right after the proof of our theorem. If the event DetextProgramming occurs, then it is possible that the signature the hint sits, a is nonellow correlation with Mysh, [L.]ma, which nodel potentially allow the signature attacker to hall only because it general that we are programming the random coracle. Assuming that the event DetextProgramming does not cross, the attacker will not be after to distinguish between a programmed response and the signatures generated via the honest signing oracle.

We now upper bound the probability that the attacker outputs a valid signature stogery without the brigge count BHDGE* are usering. Unlike our previous analysis, we only on a compression argument. FabD*Galp_i, discuss the count that the signature is valid, but we find that L_i , was not previously recorded in our list \mathcal{E} before we compared Mid($L_i = \mathcal{E}_{i} = \mathcal{E}_{i}$

Claim 5. $Pr[FaitsFind(I_n) \cup ButQuery] \le \frac{4(g_n^m + 1)}{g_{r_1}} + \frac{N^2(S + k_1)}{s}$.

We also peak the proof of China 5 after the proof of our theorem. Now we have shown that

 $\Pr\left[\mathsf{BridgeCnd}^{r,N}_{A^{(r)}_{(r),(r),r,n}}(k)=1\right]$ $\geq \Pr \left[\begin{aligned} & \mathsf{SigForgr}_{A_{\mathsf{Sig-L}_{\mathsf{p}},\mathcal{F}}^{\mathsf{T},\mathsf{K}}}(k) = 1 \right] - \Pr[\mathsf{DeterProgramming}] - \Pr[\mathsf{FullsdSign}] \\ & - \Pr[\mathsf{FullsdFind}(I_{\mathsf{p}})] - \Pr[\mathsf{BudSpary}] \end{aligned}$

 $\geq 2\tau \left[\mathrm{SigForgs}_{A_{(2r_1, \dots, r_r)}^{(N)}(X)}^{N}(X) = 1 \right] - \frac{N G_{-}^{\infty} G_{-}^{\infty} - \frac{q_{-}^{\infty}(g_{-}^{\infty} + g_{-}^{\infty})}{p} - \frac{4(g_{-}^{\infty} + 1)}{2^{k_1}} - \frac{N^2(S + k_1)}{p} \right).$ Finally, we can apply Theorem 7 to conclude that

 $\Pr\left[SigFoup_{[k]_{m,n-1}}^{n,m}(k) = 1 \right]$ $\leq \partial \left(\frac{S(d^2+N)(d^2+1N)}{2^2}\right) + \frac{Nd^2(d^2+d^2)}{2^2} + \frac{d^2(d^2+d^2)}{2^2} + \frac{N(d^2+1)}{2^2} + \frac{N^2(d+1)}{2^2}.$ Encoding Routine

46 J. Block and S. Lee

Input: an encoding function $\tau: \mathbb{Z}_g \to \mathbb{G}$, and parameters $d, R \in \mathbb{Z}^+$, where \mathbb{Z}^+ denotes the set of positive integers.

Input: an encoding function τ : Z_n → G, and parameters d, R ∈ Zⁿ, where Zⁿ denotes the set of positive integers.
 (1) Compute and write the S-bit limit ytr, v = A_m(g) into the encoding.
 (2) Write the image of τ using log [^m_m) bits into the encoding.
 (3) Write the image of τ using log [^m_m) bits into the encoding.
 (4) Initialize Table to an engagety lie. It will showe the pulse.
 (4) Expent the following d'times in total:
 (b) Chance the first N strings in the biolographical order of the image of τ that as not in the trails. Call these strings τ(x₁)..., τ(x₁), and add the point (Z_n, τ(x₁))..., τ(x_N, τ(x_N)) is the the table, where far such i i [N], X, is the intertrumsate that represents discrete ing value x₁ of τ(x₁), that the decoder does not yet know.
 (b) Kno A_m(g)σ₁, τ(x₁)..., τ(x_N),..., γ(x_N) by to R times using independent randomness from the encoder's reasonise siting in each run. Write the index τ ∈ [S] of the successful exception (i.e., it finds a BRDG2R' instance) into the encoding using log R bits. H A_m fields on all R execution, then return λ and about the entire routine.
 (c) Write a placeholder of large, zeros in the encoding, and x will be encoverize high a string that another of queries said if Radia BRDG2R' instance during the next sup.
 (d) Rerus A_m(d)σ₁, τ(x₁)..., τ(x₁)..., (x₁) using the x^m random tape. It precesses each generic group oracle query [see Handling, Rul 1(y₁, y₁) and Handling Rul(y₁) as described below and an soon as it finds a BBDG2R' instance it will mark the actual number of tord queries all in the remaining indetermination that are not per random (analyte replace them with the discrete log values (naive conocling), since the seconder shows all of z. If this is the z' entry in Tain, then it requires along the trees of a constants.
 (iv) Write the seconder incover all of z. If this

(f) Write the remaining values that are not yet in the table to the

Note that at the end of each of the d executions of $A_{\rm enc}$, we either learn the discrete log of one helds $v(\xi)$, or, we find a bridge instance in the table. In this case, we get $\log (g_{\rm enc} + \log \log g_{\rm enc})$ which of inferentians on v at v out of at most $\log R + \log g_{\rm enc} + \log \Gamma d + \log G d + \log G$

$$\log \frac{p-l}{\log R + \log g_{\mathrm{in}} + \log |\mathsf{Tabbe}|} \geq \log \frac{p-|\mathsf{Tabbe}|}{Rg_{\mathrm{in}}|\mathsf{Tabbe}|} \geq \log \frac{p-d|\mathsf{S}g_{\mathrm{in}} + N)}{Rg_{\mathrm{in}}|\mathsf{Tabbe}|}.$$

We further observe that $\log \frac{(-C)\log nN}{2\log n} \ge 1$ for $d = |\mu/(\lfloor 2B_{2m} + 1) \lceil \log n + N \rceil|$. Thus, with this value of d, we have that this not profit becomes α least 1 but for each of the d executions of A_{2m} . Hence, the total bilingth of the encoding is at

$$\begin{split} S + \log \begin{pmatrix} G_1 \\ g \end{pmatrix} &= \sum_{l=1}^p \log(p-l) - d = \log \frac{|G_1^2|}{|G_1^2| - g^2} + S - d \\ &\leq \log \frac{|G_2^2|}{|G_1^2| - g^2} + S - \frac{p}{(4R_{lin} + 1)(3g_m + N)} + 1 \\ &\leq \log \frac{|G_2^2|}{|G_1^2| - g^2|} + S - \frac{p}{4R_{lin}(g_m + N)} + 1. \end{split}$$

We want that this randomized encoding routine succeeds with probability at best 1/2. In the smoothing scatter, we can $A_{m,k}$ say to if times and see if there is any successful concertion. Since each convotion falls with probability at most c_i if we choose $H=(1+\log p_i)/c_i$, then all H excentions all fail with the probability at most

$$(1-c)^R \le e^{-cR} \le 2^{-cR} \le 2^{-(-\log p)} = \frac{1}{2p} \le \frac{N}{2p}.$$

ding over the $\frac{p}{n}$ different executions of A_{nn} , the probability

$$(1-c)^{\alpha} \leq e^{-c \cdot \alpha} \leq 2^{-c \cdot \alpha} \leq 2^{-c \cdot \alpha} = \frac{c}{2^{\alpha}} \leq \frac{c}{2^{\alpha}}.$$

Usion bounding over the $\frac{c}{2}$ different exercision of A_{n} , the probability that the encoding rowtine fields in at most $1/2$. With this value of R , the encoding length is at most
$$\log \frac{|G|}{|G|-p|} + S + 1 - \frac{cp}{4q_{nc}(q_{nc} + N)(\log p + 1)}.$$

which completes the proof. Reminder of Theorem 5. Let $H=(K_{\mathbb{Q}}, \operatorname{Sip}, \operatorname{Vb}_{\mathbb{Q}})$ be a trap-profited Schner-siparium reduces can $p>0^n$ be a prime remine. Let $N\in\mathbb{N}$ is the a parameter and $(X_{\mathbb{Q}}^n, X_{\mathbb{Q}}^n)$ be a pair of pennic algorithm with one considing map $r: Z_{\mathbb{Q}} = G$ such that $X_{\mathbb{Q}}^n$ makes at most $X_{\mathbb{Q}}^n$ spectrum to the random sense in $([0,1]^n)=([0,1]^n)$ and onlysts an S-let hind $G:_{\mathbb{Q}_p}$ such as $A_{\mathbb{Q}_p}^n$ makes at most $X_{\mathbb{Q}_p}^n$ in $X_{\mathbb{$

$$\begin{split} & \Pr\left[\operatorname{SigFugp}_{\mathcal{L}_{\operatorname{alo}_{-1}, \mathcal{L}}^{(k)}}^{\mathcal{L}_{\operatorname{alo}_{-1}, \mathcal{L}}^{(k)}}(k) = 1 \right] \leq \varepsilon, \text{ with} \\ & \varepsilon = \tilde{O}\left(\operatorname{SigC+N}(\operatorname{SigC+N}) \right) + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} \right) + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} \right) + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} \right) + \operatorname{NiG-NiC} + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) + \operatorname{NiG-NiC} \right) \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) \\ \\ \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) \\ \\ \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right) \\ \\ \\ & = O\left(\operatorname{NiG-NiC}(\operatorname{NiG-NiC}) \right)$$

54 J. Blocki and S. Lee

Similar to Theorem 7, if
$$q_i^m \ge 10N(1 + 2 \log p)$$
 and $S \ge 10 \log(3p)$, then

$$Pr \left[2q_i^m \exp_{\alpha_{ij}^m \alpha_{ij} \alpha_{ij}^m \beta_{ij}^m \beta_{ij}^m \beta_{ij}^m + q_i^m + q_i^m \beta_{ij}^m + q_i^m \beta_{ij}^m + q_i^m + q_i^m \beta_{ij}^m + q_i^m + q_$$

Reminder of Claim 4. $Pr[DenxtPegramming] \le \frac{N_B^{ent}q^{th}}{d}$.

Proof of Claim 4: Let $I_i = \operatorname{Pow}[g, n_i]$ be the value generated during the i^* query to the signing eracle. Let $B_{i,j}$ denote the had exent that the proposessing attacker previously architector architector p and I_i are advected maximum, we have $\operatorname{Po}[B_{i,j}] \leq a_i^{m_i} p^{k_i}$. But now define the event $\operatorname{Deta}(P) = \operatorname{Po}[B_{i,j}] \leq a_i^{m_i} p^{k_i}$. By now define the event $\operatorname{Deta}(P) = \operatorname{Po}[B_{i,j}] \leq a_i^{m_i} p^{k_i}$. By now define the event $\operatorname{Deta}(P) = \operatorname{Pow}[B_{i,j}] \leq a_i^{m_i} p^{k_i}$.

$$\Pr[\mathsf{DetectProgramming}] = \Pr[\bot_{i,j}B_{i,j}] \leq \sum_{i} \Pr[B_{i,j}] \leq \frac{Nq_{i}^mq_{i}^m}{p_{i}^{2m}}. \qquad \Box$$

Resolution of Claims 5. $Pr[fultoFind(I_n),distQuery] \le \frac{d(g_n^m+1)}{2^{n}} + \frac{N^2(S+k_2)}{2^{n}}$,

Proof of Claim is: Fixing
$$\tau$$
 and H , and for some parameter t (which we will determine later), we define $\varepsilon_{F,t,B}$ to be
$$\varepsilon_{F,t,B} := \min_{T \in T_{t} \setminus \{t,B\}} P_{t}[Tainofind(|t_{t}|) \cup BindQuern(|t_{t}|)]$$

where the probability is taken over the random selection of $x_1, \dots, x_N \in \mathbb{Z}_p \setminus Y$ and the random coins of $A_{n_1, n_2, \dots}^{(n)}$. We can segme that rannoting $N : n \mid NY$ points does not impact this probability, i.e., $c_{N,N} \approx c_{N,N}^2$, where $c_{N,N}^2$ is the same probability when $x_1, \dots, x_N \in \mathbb{Z}_p$ are charm without any root distribution, $c_{N,N}^2 \le c_{N,N} + N^2(p)$ where the term $N^2(p)$ upper bounds the probability that sample some point $x_1 \in Y$.

e-extract f input/output predictions, undom min when sampling d* and q*:

(ii) For $i \in [t]$, sample $t' = (x'_1, \dots, x'_N)$ subject to the restriction that $x'_j \neq x'_j$. for any pair $(i, j) \neq (t', j')$, ..., $x'_N = (t', i') = (t', i')$. (ii) Pick $q' \in [0, \frac{n}{2}]$ uniformly at random. (ii) If q' = 0, then wait for the juttempted) found signature $x_i = (x_i, x_i)$ to be surput, enument $L = r(x_i - x_i')$, and output the prediction $H(r(x'_i)) \in L_1(m_i)$.

On the Walti-Corr Security of Short Schoorr Signatures with Preprocessing 55

(ii) If instead q'>0, then we simulate $A^{\rm sig}_{m,m',n}$ satisf the query q' to the random sensite. At this points, the query has the form $H(gh_p[f]|n)$ for some f such that $\{f_n, f_n\} \in \mathcal{L}'$. In this case, we can extract c from \mathcal{L}' and conjust the prediction $H(gh_p[f]|m) = c$.

During each iterations i, we output a correct input/output pair with probability at least $t_{T_p,m}/t_0^{2m}+1$. Thus, the procedure above correctly outputs t input/output pairs with probability at least $t_{T_p,m}/t_0^{2m}+1$. Thus, the procedure above correctly outputs t input/output pairs with proceduring at least $(t_{T_p,m}/t_0^{2m}+1)^m$. Let S accessing describe an event that the experiment above correctly outputs t exercise impulsival part pairs t exercise impulsival part pairs t exists at uncertainty when τ and θ are pictod randomly. Now let $\tau_F = R_{r,m}/\tau_{F,r,m}$ and suppose that $t_F > 4/4g_m^{2m}+1/2^{-m}$, for contendeding, then we can use blackers inequality to argue that

$$\begin{split} \Pr_{i,k} \left[i_{F,j,0} > \frac{\log(t^k + 1)}{2^{k_k}} \right] &= 1 - \Pr_{i,k} \left[i_{F,j,0} \leq \frac{2(\log^k - 1)}{2^{k_k}} \right] \\ &= 1 - \Pr_{i,0} \left[1 - i_{F,j,0} \geq 1 - \frac{2(\log^k + 1)}{2^{k_k}} \right] \\ &\geq 1 - \frac{1 - i_F}{1 - 2(g^k + 1)^{2-k_k}} \end{split}$$

 $> \frac{\epsilon_F/2}{1 - \epsilon_F/2} \ge \frac{\epsilon_F}{2}$. Thus, if we pick τ and H randomly and run the above procedure, we will succoed with probability at least

$$\Pr[\text{SummedExp}] \ge \frac{r_2r}{3} \left(\frac{(r_1,\mu)}{d_1^{r_1}+1} \right)^t \ge \frac{r_2r}{3} 2^{(1-r_1)t} > 3(q_1^{m}+1)2^{-r_1}2^{(1-r_1)t},$$

 $P(SucceedExpl \le 2^{-\alpha_i t + \delta})$ Picking $t = S + k_1$, we derive a contradiction, since, with this value of t we have

 $\mathbb{F}[g_n^m + \mathbb{E}[2^{-k_1\beta-k_1^m+\delta}] + \ell < \Pr[SucceedExp] \leq 2^{-k_1\beta-k_1^m+\delta},$ The contradiction comes from the assumption that $z_F > 4(g_b^{aa} + 1)2^{-b_c}$. Thus, we have

> $c_{\sigma}^{*} := \Pr(\mathsf{FaltoFind}(I_{\sigma}) \cup \mathsf{SinfQuery})$ $= \mathbb{E}_{r[n]}[c'_{F(r)n}]$ $\leq \mathbb{E}_{r[n]}[c_{F(r)n} + \frac{N^2\{S + k_1\}}{p}]$ $= c_F + \frac{N^2(S + k_1)}{p} \le \frac{4(q_2^m + 1)}{2^{k_1}} + \frac{N^2(S + k_1)}{p}.$

Lemma 4 has appeared in prior work in various forms. To the best of our knowledge, the original usage is from [INWWI] though our statement is closer to a form from [INWII]. Since we replease the lemma elightly, we include a proof of Lemma 4 below for completeness.

Definition 4 (b-bit prediction game). Let B be a uniformly readon let sing and let A be an algorithm that receives a limit $h = f(B) \in B$ which may depend orbitrarily as B and can additionally query B at specific indices halow colouring unifors i_1, \dots, i_n and bits i_1, \dots, i_n . We say that A wins the bits prediction game if for all $j \le k$ or have $B(p_j) = b_j$ and A did not previously query for $B(p_j)$.

Lemma 4 ([DKW11,BHK*16]), Jup attacker A wise the t-bit prediction game with probability at most $[M/2^k]$.

Proof. Let Success, a denote the starder's success probability when h=f(H) depends on B. Suppose for contradiction that $P(Success, g) > |M|^{\alpha-1}$, then consider the algorithm A which takes no birst, samples $h \in H$ uniformly, and simulator A with birst h. We have $\Pr[\operatorname{Summ}_{A^{\prime}}] \geq \Pr[h = f(B)] \Pr[\operatorname{Summ}_{A}] > \frac{1}{|\mathcal{M}|} |B| 2^{-k} = 2^{-k}.$ To obtain a contradiction, we observe that A' concends with probability at most T^{-k} . In particular, A' starts with no hint and outputs i_1, \ldots, i_k and bits b_1, \ldots, b_k such that $B(j_i)$ has not been queried for all $j \leq k$. In this case, we can size such $B(j_i)$ are uniformly random bit samplest after A' outputs. Thus, $Pr(bj \leq k, b_j = B(j_i)) = T^{-k}$, which implies that $Pr(\mathsf{noness}_{A'}) \leq T^{-k}$.

Beninder of Thorren 8. The Chain-Pidersen-FDB signature whene is $\left(S, q_0, q_0, q_0, \mathcal{Q}\left(\frac{\pi - \pi}{2}\right)\right)$ MU-UF-CMA secure under the generic group model of prime order p is 2^{24} and the programmable random aracle model, where q denotes the total number of queries made by an adversary.

From Storick of Theorem 2. Let H be the Chaum-Pederson-IDH signature achieve. We follow a similar reduction in in Theorem 6 using the signature achieve, we follow a similar reduction in in Theorem 6 using the signature substance, but follows a first reduction in in Theorem 6 using the signating oracle without knowledge of the secret key x_i in Figure 3 (top). Note that the exercise standing public key is $pk_j = r(x_i)$. We have reduce that x_i and x_i of all x_i of the form $H(k)(p(x_i))$ we can onsere that x_i and x_i of all x_i of x_i on the standing x_i of x_i or x_i or x_i of x_i or x_i or

we call $\operatorname{Hag}(f)$ before corrying the random crude. Now define a subset $\widetilde{\mathcal{E}}\subset\mathcal{E}$ as the set of tupin $(a,d,b)\in \mathbb{G}\times\mathbb{Z}_p^N\times\mathbb{Z}_p$ such that δ has exactly one nonzero element. Now we call a random oracle query x=(I|m) "bad" if $\Re(x)=-\overline{a}$

Bounder of Theorem 7. Let $p>2^{2k}$ be a prime number and $N\in\mathbb{N}$ be a permeter. Let (A_{nn},A_{nn}) be a pair of provine algorithms with an encoding map $r:\mathbb{R}_p\to 0$ is such that A_{nn} extent on S but that and A_{nn} matrix at most $q^n=q^n(k)$ queries to the practic group sensits. Then

 $\Pr\left[\text{BridgeChal}_{\mathcal{A}_{0,D,r}}^{r,N}\left(\delta\right)=1\right]\leq\tilde{\mathcal{O}}\left(\frac{S(g_{1}^{m}+N)(g_{2}^{m}+2N)}{n}\right),$

where the randomness is taken ever the sciention of ε , the random coins of A_{mn} and the random coins used by the challenger in the bridge gener (like hird tht. = $A_m^2(\underline{\omega})$) is related independently of the random coins used by the challenger). In particular, if $q_1^{mn} \geq 10N(1+2\log p)$ and $S \geq 10\log(|q_1|)$, then $\Pr\left[BridgeChal^{1/2}_{A_{m,m_{\alpha}}}(\lambda) = 1 \right] \leq \frac{14.5(g^{m})^{2}\log p}{n}.$

From of Theorem 7: We follow the same idea from [CR18, Theorem 2], which shows the relationship between the size of the limit S and the probability x that can win the multi-near heigh-finding game. So that a map τ is good if $(A_{\mu\nu}, A_{\mu\nu})$ where the multi-near heigh-finding game with probability at least z/2on τ . That is, τ is good if we have

 $\Pr\left[\mathsf{BridgeChaf}_{A_{m,\mathsf{str.}}}^{r,X}(k) = 1\right] \geq \frac{e}{2},$

where the probability is taken over the selection of $\mathcal{S} = (x_1, \dots, x_N) \in \mathbb{Z}_+^N$, the random exists of A_{mn} , and the random exists used by the challenger in the bridge game (the hint str. $-A_m^N(y)$) is observed independently of the candiom exists used by the challenger).

Let $T = \{v_1, v_{n-1}\}$ be the set of good labeling maps. Then by a standard averaging argument $(2A_{mn})$, Lorentz A.PE), as (x/2)-features of hipothem mappings from \mathbb{Z}_p to G are good. One could also observe that the number of injective mappings from \mathbb{Z}_p to G is $[G]/(|G| - p)\ell$, which implies that $|T| \geq (s/2) - |G|/(|G| - p)\ell$.



Handling $Halt(y_1,y_2)$: (1) If either of η_1 or η_2 is not in the image of τ , reply \bot and continue to

(a) in extent of query.
(b) if either of q₁, or q₂ is not in the table, then this is a β-not query input.
For each such argument is ∈ (q₁, q₂), add the pair (Ex.q(q), a) to the table and write a to the exceeding using log(p − 0) bits, where ℓ is the number of labeles already in the table.
(3) Otherwise, look up the taples (⟨1, q₁⟩, ⟨1_p, q_p) in the table where ℓ₁ = ℓ₁(X₁, ..., X_n) and ℓ₁ = ℓ₁(X₁, ..., X_n) are linear polynomials of N indiscensinates X₁, ..., X_n, and compute f₁ + f₂.
(a) If (f₁ + f₂, Rult(q₁, q₂)) is alwardy in the table, simply reply with Rult(q₁, q₂).
(b) If (f₂ + f₃, Rult(q₁, q₃)) is not in the table, then add Rult(q₁, q₃).

(ii) If (f) ∈ f_s = Mol*(η_s, η_s) is not in the table, then add Mol*(η_s, η_b) in the encoding and updy with Mol*(η_s, η_b). White Mol*(η_s, η_b) is to the encoding and updy with Mol*(η_s, η_b). White Mol*(η_s, η_b) is the encoding requires log(g) = f_b bins, where f is the manuface of labels absently in the table.
(ii) If Mol*(η_s, η_b) is in the table but its corresponding discount log value in the table is a linear polynomial f = f(X_s,..., X_s) such that f is not identical to f_s + f_s (i.e., the coefficients for X_s) are not all the namely, then ensemble the suply on this query as a pointer to the table entry (f/Nol*(η_s, η_s)) and add this pointer to the encoding. Then use the equation f = f_s + g_s is drive an equation X_s = g(X_s,...,X_s,...,X_s,...,X_s). For some j and a linear polynomial g of X₁,...,X_s except for X₁, and replace X_s by g(X_s,...,X_s,...,X_s).

On the Multi-User Security of Short Schner Signatures with Proprocessing 52

 $A_{min}^{max}(g)$ is solveted independently of the random series used by it. In particular, if $q_1^m \ge 10N(1 + 2 \log p)$ and $S \ge 16 \log(3p)$, then $\varepsilon = \frac{14S(\underline{e_i^{-1}}^2\log p}{\mu} + \frac{N_i\underline{e_i^{-1}}\underline{e_i^{-1}}}{\mu} + \frac{q_i^{-1}(\underline{e_i^{-1}} + \underline{e_i^{-1}})}{\mu} + \frac{4(\underline{e_i^{-1}} + 1)}{\mu} + \frac{N^2(S + k_1)}{\mu}.$

Proof of Theorem 6: Given a generic obversacy with proprocessing (A^{m}_{m}, A^{m}_{m}) attacking Schoorr signature obsers, we construct the following efficient generic algorithm with proprocessing (A^{m}_{m}, A^{m}_{m}) which true to accord in the 1-cut-of-N generic $BBDGL^{N}$ —finding game $BridgeDud^{N}_{A^{m}_{m}, m-1}(0, d)$.

Algorithm $(A_{\operatorname{tripp}}^{m}, A_{\operatorname{tripp}}^{m})$: The algorithm is given $p, p = r(1), pk_i = r(x_i), 1 \le i \le N$ as input.

part/contpart points observed during unline processing. 3. $A_{ijk}^{(k)}$ takes the thint are, a and shiftalizes the fact $C = \{(\tau(1), \vec{0}, 1), (pk_i, \vec{u}_i, 0)\}$ for $1 \le i \le N\}$, and thus $A_{ijk}^{(k)}$ with the laber are, and a number of access to the generic group oracles for $(0, (0, 1), (pk_i, \vec{u}_i, 1), (pk_i, \vec{u}_i, 1), (pk_i, \vec{u}_i, 1), (pk_i, \vec{u}_i, 1), (pk_i, 1)$ f a generic group query during the online phase appears in the list \mathcal{L} . We

and add in 0.01 to 2. (b) Whenever $A_{\bf kq}^{\rm o}$ submits a query 4 to the generic group oracle law(-):

to \mathcal{L} .

Otherwise, $(\mathbf{a}, d, \mathbf{b}) \in \mathcal{L}$ for some \mathcal{L} and \mathbf{b} . Then we query $\ker(\mathbf{a}) = \pi^* (-d \cdot F - \mathbf{b})$, subject the result and $\operatorname{add}(\pi^* (-f - \mathbf{b}), -d, -d) \in \mathcal{L}$. In (\mathbf{c}) . Whenever, $\mathbf{d}_{\mathbf{c}}^*$ enter \mathbf{d}_{\mathbf

 $\begin{aligned} & \operatorname{Relation}_{A}(k) = r((k_k + k_k) \cdot \mathcal{F} + k_k + k_k) \text{ and add} \left(r((k_k + k_k) \cdot \mathcal{F} + k_k + k_k) \cdot k_k \cdot k_k \right) \cdot \mathcal{F}_{A} + k_k \cdot k_k \cdot$

We introduce Lemma 3 which has been adopted from Abadi et al. [AFK87]

Lemma 3. For a prime p, let (A_{mn}, A_m) be a pair of generic algorithms for \mathbb{Z}_p on \mathbb{Q} with an examining map $r: \mathbb{Z}_p \to \mathbb{Q}$ such that A_{mn} outputs an θ -bit hast θ th, makes at most q_m proving group smoot queries. Then there exists a generic algorithm A_m that makes at most $q_m = 1/2\mathbb{N} \log p + N$ perceive group equals queries, and, for energy $r: \mathbb{Z}_p \to \mathbb{G}$, if $\mathbb{P}(r, A_m) \mathbb{R}(\log p \mathbb{C} M_{A_m}^{r, A_m}(k, \ell) = 1) \geq \varepsilon$, then for energy $\vec{x} = (x_1, \dots, x_N) \in \mathbb{Z}_p^N$, $\Pr_{X_{ij}} | \text{BridgeChal}_{X_{ij}, \text{str.}}^{(S)}(\hat{x}, \vec{x}) = 1 | \geq \varepsilon$. Proof. Algorithm $A'_{rs}(\operatorname{str.}, \tau(x_1), \dots, \tau(x_N))$ executes the following:

Observe that during the convention of $A_{i,i}$, we run $A_{i,j}$ on $(r[x_i,x_1],\dots,r[x_k-x_k])$, which is the image of a uniformly random point in \mathbb{Z}_i^n . Since we assume that the bridge-finding genes with $A_{i,i}$ moreodo with probability at least c over the random selection of $\mathcal{E} = \{x_1,\dots,x_k\} \in \mathbb{Z}_q^n$ and its coins, we can conclude that the bridge-finding genes with $A_{i,i}$ since reasonable with probability at least c and yours the selection of its coins.

Now we are back to the proof of Thuscon 7. Lemma 3 implies that there ists a pair of generic algorithms (A_{mn}, A'_{mn}) such that for every $\tau \in T$ and every

 $\log \frac{|G|!}{|G|-p|!} + S + 1 - \frac{(\epsilon/2|p|}{6q_p^{pr'}(q_p^{pr'}+N)(\log p + 1)}.$ where the mending scheme works with probability at least 1/2. The incompressibility argument* of De et al. $||\mathbf{UTTH}||$ may that this length must be at least $\log |T| - \log 2$. Hence, we have that

 $\log\frac{|G|}{(|G|-p)!}+S+1-\frac{(\epsilon/\mathbb{E}p)}{6q^{\prime\prime}(q^{\prime\prime}+N)(\log p+1)}\geq\log\frac{|G|}{(|G|-p)!}-\log\frac{4}{\epsilon},$

not identical to f (i.e., the coefficients for X_i 's are not all the same), then encode the regit to this query as a pointer to the table entry $(f, \operatorname{Im}(q))$ and add this pointer to the modeling. Then use the equation f = -f to derive an equation $X_i = g(X_1, \dots, X_{f+1}, \dots, X_{f+1})$ by the same j and a linear polynomial g of X_i, \dots, X_{f+1} except for X_i , and epilace X_i by $g(X_1, \dots, X_{f+1}, \dots, X_{f+1})$ in the table. execution of the algorithm and indicate the surly stop by writing the actual number of question $q^* \le q_{an}$ into its placeholder above.

The decoding routine is given the encoded string and recovers τ as follows:

Initialize Table (input/output pairs for r) as an empty list.
 Entract r(1) from the encoding and add (1, r(1)) to table.
 Entract the filtering of times in total.
 Choose the first N strings in the lexicographics order of the image of that are not in Table. Call these strings q₁... q_N and add the pairs N₁, q₁,..., q_N, and add the indeterminates that represent the discrete log of q_i's for i = 1,....

the indeterminates that supersecut the discrete log of q_i 's for $i = 1, \dots, N$.

(b) Decode $\sigma^* \in [R]$ after reading $\log R$ bits from the encoding.

(c) Decode $\sigma^* \in [g_{i+1}]$ after reading $\log g_{i+1}$ bits from the encoding.

(d) Ross $A_{ij}(k,te_{ij}, n_{i+1}, \dots, n_{i+1})$ for q^* specifies using the e^{-int} sendom tops allocated for this instance of A_{ij} .

i. If A_{ijk} unders the query $\operatorname{Sol} 1(g_{i}, p_{ij})$:

ii. If either a_i or a_i is not in the image of τ , reply i.

B. If either a_i or a_i is not in the image of τ , but not in the table, then add either $\operatorname{Sol} (S_i, a_i)$ to the table, where i and j are the smallest integers such that S_i and S_j are the fresh indeterminate in the table.

C. Smach for the table and find the pairs (j, a_i) and (f_0, a_i) , and excepted the linear polynomial $f_1 + f_0$.

(i) If (f_1, a_j) , we is already in the table, then ruply with m and contains to the sent query.

(2) If there is no such m is the table, and if this is not the last $(p^{**})^{**}$ query of this ensembles, then read $\log p_i = 1$ is to from the exacteding, where l is the summer of lakeds in the table, and discode the bits to estipate m. Reply with m, and add $(l_i + f_{j,i}, n_i)$ to the pairs of containing m in the table, we have a such m in the table.

i. Pub a_i, c_i randomly and compute $I_i = \pi(s_i - x_j c_i) = \Re s \ln(s_i, -re, j)$, where $s_i = \operatorname{Per}(g, s_i)$.

ii. If $\Re g s_i [I_i] m_i$ has been precised unionly quotied, then return A.

iii. Otherwise, program $\operatorname{High}_{B_i} [I_i] m_i) = s_i$ and stars $\sigma_i = (s_i, c_i)$.

We smooth that a side effect of quoying the Eqs. such is the addition of the randomly A of A in A in

Int. No.11.

(ii) if at any point we have some string q such that $[q, d, b] \in \mathcal{L}$ and $[q, d, d] \in \mathcal{L}$ for $[d, b] \notin (\mathcal{L}d)$ then we can immediately have a $BROCC^{N}$ instance (x | (d - d), d - d), (d - d), (

that $\forall \Gamma[g]_n, m_n, \sigma_n] = 1$. 5. Compute $\tau[-\epsilon_1, \mu_n] = 3\pi \tau(Pow(\tau(x_n), \epsilon_n))$. This will ensure that the dismens $(\tau[-\epsilon_1, \mu_n]_n) - \mu_n h_n)$ and $[\tau[\epsilon_n, \mu_n]_n + \mu_n h_n]$ are both added to \mathcal{L} . 6. Compute $h_n = Pow[g, h_n]$ to course that $(h_n, h_n) - \mu_n h_n h_n h_n$ which ensures that $(L_n, \tau[\epsilon_n, \mu_n]) = \mathcal{L}$. 7. Fixedy, compute $L_n = 8h h(h_n, \tau[-\epsilon_n, \mu_n]) = \tau(h_n - x_n e_n)$ which ensures that $(L_n, -\epsilon_n h_n, h_n) \in \mathcal{L}$.

Analysis. We first remark that if the signature is valid then we must have

 $\Pr\left[\mathsf{SigFogr}^{*,\mathbb{R}}_{A^{\mathsf{Sig}}_{\mathrm{cons},\mathcal{S}},\mathcal{S}}(k) = 1\right] - \Pr(\mathsf{DetextProgramming}) - \Pr(\mathsf{Fulledign}),$

where $\Pr[SigForgr^{*N}_{L^2_{12},n_{12},n}(t)=1]$ denotes the probability that the attacker is successful when pinying with the seal signing cracks.

Fallstfigs is the exect where our reduction sutputs \bot in Sep 2(d) due signing oracle shines, i.e., thering some query t, we generate L, and that that the random rando query H_0 , $L[\exists m]$, was made previously during the sulner phase. As believe, we can august that

 $\Pr[\mathsf{Fullsofign}] \leq \frac{q_1^{\mathsf{pr}}(q_1^{\mathsf{pr}} + q_1^{\mathsf{pr}})}{2}$

i.e., see Claim 1.
Insulvely. DemotPugganesing denotes the event that the candom oracle query M(pt, [L]m.) was made in the offline phase. Now we have the following chim to upper bound the probability of the event OutschPugganning:

 $S \ge \frac{cp}{6(q_1^m + 2N\log p + N)(q_1^m + 2N\log p + 2N)(\log p + 1)} - \log \frac{\pi}{\epsilon}$ Without has of generality, we may assume that $\varepsilon \geq 1/p$, since the probability to find a BHDGE⁰ instance is not lower than solving 1-out-of-N descrete log problem (see Corollary 1), which is also not hover than 1/p when guessing them randomly, Brance, we have obserted by $\frac{\pi}{2} \leq \log(3p)$ and we get

 $6\left(S+\log(8p)\right)(|g_0^m+2N\log p+N)(g_1^m+2N\log p+2N)(\log p+1)\geq \epsilon p,$

 $z \le \frac{6}{a}(S + \log(8p))(g_0^m + N + 2N \log p)(g_0^m + 2N + 2N \log p)(\log p + 1)$ $= \tilde{\mathcal{O}}\left(\frac{S(q_1^m+N)(q_1^m+2N)}{p}\right),$

i.e., if the size of the hint is bounded then the probability of winning the 1-out of N generic bridge-finding game is also bounded correspondingly. In particular, if $q_n^n \geq 16N(1+2\log p)$ and $S \geq 10\log(3p)$, then we observe that $z \le \frac{6}{a}(S + \log(8p))(g_0^m + N + 2N \log p)(g_0^m + 2N + 2N \log p)(\log p + 1)$

 $\leq \frac{6}{p}(1.18)(1.1q^m)(1.3q^m)(1.5\log p) \leq \frac{145(q^m)^2\log p}{p}$, where we have $\log p + 1 \le 1.5 \log p$ because $p > 2^{20}$ implies $\log p > 2k$ and $\log p + 1 \le (1 + 1/(2k)) (\log p \le 1.5 \log p$.

Remains due of Lemma 1. Let G be the set of binary strings of length ℓ such that $T' \geq p$ for a prime p. Let $T = \{r_1, r_2, \dots\}$ be a subset of the labeling functions from Σ_n to G. Let (A_{nn}, A_{nn}) be a pair of generic algorithms for Σ_n on G such that f or every $e \in T$ and every $d = \{r_1, \dots, r_d\}$ of $\Sigma_n^{n_d}$, A_{n-1} where on S-bit advice string, A_{nn} mains at most q_{nn} oracle queries, and $\{A_{nn}, A_{nn}\}$ satisfy $\text{Pr}_{A_m}\left[\text{BridgeChar}_{A_{m,m}}^{(N)}(0,\delta) = 1\right] \ge \varepsilon$, where $\text{str}_s = A_{ss}^{\text{tot}}(\tau(0))$. Thus, five crisis a randomized encoding scheme that compresses elements of T to bilitrings of length at most

 $\log \frac{|\Omega|}{(|\Omega|-p)!} + S + 1 - \frac{\epsilon p}{6g_{ac}(g_{ac}+N)(\log p + 1)}.$ and records with probability at least 1/2.

Proof of Lemma 2: The proof works largely the same as it from [CK10] enough for some modifications. In the proof of [CK10], they build an encoding and a

On the Multi-Corr Security of Short Schoor Signatures with Prepresenting 69

outry (S_n, ϵ) to the table, where i is the smallest integer such that S_i is the fresh indeterminate in the table. C. Search for the table and find the pair (f, a), and compute

the linear polynomial -f. (1) if (-f, m) is sleenly in the table, then reply with m and continue to the next query. (2) if there is no such m in the table, and if this is not the (2) If there is no couch w in the table, and if this is not the last (µ⁻¹) query of this exacution, then mud large −1) him from the encoding, where ℓ is the number of hileds in the table, and decode the bits to output m. Now spily with m, and add (−f, n) to the table and continues to the next query. (3) If there is no such w in the table, and if this is the last (q⁺¹) query, then we know that we have a bridge instance here. Thus, read a log [Table hit pointer from the encoding and search for the entry is the table with his pointer, any (f, m). Solve the equation f = −f mod p in the first indexensions f is in the oparities. Replace every S is the polynomials in the table with the solution of the equation so that there is no longer S in the exist of the continue table.
iii. Broad the values of all the remaining indeterminates as they appear in the table.

The total encoding length will be calculated as follows:

where τ (S bits), the encoding of the image of τ (log $\binom{m}{2}$) bits), the index τ' which denotes the succonduct encention of A_{mc} (ding R bits), the section amoster of total quasitor τ' (ding m_c bits), for the t^m entry that is added to the table $(0 \le l < |Tabin|)$, if the entry τ corresponds to an indeterminant that has been resolved by finding a BRDGE² instance (at most log (Table bits), τ otherwise, log(τ − t) bits, and the remaining distorate by quives, encoded using log(τ − t) bits each, where

: the remaining discrete log values, encoded using $\log(p-l)$ bits each, where $l\in \{Table|,\ldots,p-1\}$.

On the Multi-User Security of Short Schner Signatures with Proprocessing 50 Claim 4. $Pr[DenstProgramming] \le \frac{N q_{ij}^{m} q_{ij}^{m}}{\sigma^{2}}$.

the regardene attacker to half early become it general that we are programming the random stacks. Assuming that the event DetailTraguaraning does not occur, the attacker will not be after the distinguish between a programmed response and the signatures generated via the honorst signing search. We now appear become the probability that the attacker outputs a valid signature appear because the probability that the attacker outputs a valid signature flaggery without the bridge event $BRDGE^{\infty}$ occurring. Unlike our previous analysis, we rely on a compression argument, $F_BbDGalf_{1,1}^{\infty}$ denotes the overtime that the signature is valid, but we find that L_{∞} was not previously recorded in our list \mathcal{E} before we computed $Bab(u_{1,1}^{\infty}, v_{1,1}^{\infty}, v_{1,1}^{\infty}, v_{1,1}^{\infty}, v_{1,1}^{\infty})$, below that \mathcal{E} is such a previously queried $H_{Bal}^{\infty}(L_{1,1}^{\infty}, v_{1,1}^{\infty}, v_{1,1}$

Claim 5. $\Pr[FaltoFind(I_n) \cup EurQuery] \le \frac{d(q_n^m + 1)}{p^n} + \frac{N^2(S + k_1)}{p}$

We also peak the proof of $\frac{1}{2}$ ofter the proof of our theorem. Now we see shows that

 $Pr\left[BridgeOni_{A_{O(q_1,r_{r_1,q})}}^{r_1N}(k) = 1\right]$ $\geq \Pr\left[\text{SigForge}_{A_{m_{n,N}}^{m},\mathcal{X}}^{*,N}(k) = 1\right] - \Pr[\text{DetectProgramming}] - \Pr[\text{FaltaSign}]$

- Pr(FallsoFind(I_)) - Pr(BadQuery) $\geq \Pr\left[\operatorname{SigFuge}_{A_{n_{1},n_{1},p}^{1,N},B}^{1,N}(k) = 1 \right] = \frac{N_{n_{1}}^{N}g_{1}^{N}}{p^{2}} - \frac{g_{1}^{N}(g_{1}^{N} + g_{2}^{N})}{p} - \frac{4(g_{1}^{N} + 1)}{2^{N}} - \frac{N^{N}(S + k_{1})}{p},$ Finally, we can apply Theorem 7 to conclude that

 $\Pr \left[SigFoup_{A_{m_{m,m}}^{(i)},H}^{i,\pi}(k) = 1 \right]$ $\leq \mathcal{O}\left(\frac{N(q^n+N)(q^n+1N)}{p}\right) + \frac{N(q^n-q^n)}{p^n} + \frac{q^n(q^n+q^n)}{p} + \frac{N(q^n+1)}{2^{n}} + \frac{N^n(q+1)}{2^{n}}$

routine takes as input an encoding function $\tau:\mathbb{Z}_0\to \mathbb{G}$ and a random binary string τ , and outputs a compression of τ . The denoding soutine reverts this operation; it values as inputs a compressation of τ and the same random string τ as used in the encoding routine, and outputs the original τ . One

Input: an encoding function $\tau:\mathbb{Z}_p\to \mathbb{G},$ and parameters $d,R\in\mathbb{Z}^+,$ where \mathbb{Z}^+ denotes the set of positive integers. Compute and write the S-bit limit str. v- A_{pri}(g) into the encoding.

(2) Write the image of τ using log (⁽ⁿ⁾_g) bits into the encoding.
(3) Initialize Table to an empty list. In will store the pairs (g, τ |g|), i.e., an element in the image of τ and its discrete log value.

dements in the image of r and its discrete log value, (4). Repeat the following of times in total (4). Repeat the following of times in total (4). Choose the following of times in total (4). Of these obtains N strings in the indexequations and r of that are not in the table. On these obtains $r(x_1, \dots, r(x_N))$ and add the pasies $(X_1, r(x_1)), \dots, (X_N, r(x_N))$ in the table, where for each $t \in [N]$, X_i is the indextrationable that represents districted by value x_i of $r(x_i), \dots, r(x_N)$, $r(x_N)$ to R times using independent randomness from the encoder r random setting in each r on r of R in the index $r^* \in [R]$ of the successful exercision (x_i, y_i) finds a R RDORF instance) into the encoding using p(R) that R A_i finite on all R execution, then return i, and about the entire routine.

(b) Write a placeholded or d $p(y_i)$, zeros in the encoding, and it will be conservable when r is the an anomalous objects of the conservable objects of the conservable r in the encoding, and it will be instance obtains the next size.

the table are constants.

) Write the remaining values that are not pet in the table to the

preprocessing attacks?

gnatures are secure!

On the Hubi-Corr Security of Short Schnerr Signatures with Prepresenting 55 (6) If instead q' > 0, then we simulate $A^{m}_{m,m+1}$ until the query q' to the candisatorselle. At this point, the query has the form $H(pk_{j}[f]|m)$ for some f such that $(f, ck_{j}, g', g') \in \mathcal{L}'$ be this rank, we can extract c from \mathcal{L}' and comput the prediction $H(pk_{j}, g')(m) = c.$

 $\Pr_{i,n} \left[\epsilon_{F_i \cap B} > \frac{2(q_i^m + 1)}{2^{k_i}} \right] = 1 - \Pr_{i \in B} \left[\epsilon_{F_i \cap B} \le \frac{2(q_i^m + 1)}{2^{k_i}} \right]$

 $=1-\Pr_{r,s}\left[1-c_{F,r,m}\geq 1-\frac{2(q_{r}^{m}+1)}{2^{r_{r}}}\right]$

 $\geq 1 - \frac{1 - r_f}{1 - 2(q_s^m + 1)2^{-k_s}}$

 $> \frac{\epsilon_F/2}{1 - \epsilon_F/2} \ge \frac{\epsilon_F}{2}$.

Thus, if we pick τ and H randomly and run the above procedure, we will succoed with probability at least

 $\Pr[\mathsf{SucceedExp}] \geq \frac{cy}{3} \left(\frac{cy_{1:H}}{q_{2:}^{2}+1} \right)^{r} \geq \frac{cy}{3} 2^{(1-c_{1})t} > 2(q_{1}^{m}+1)2^{-c_{2}} 2^{(1-c_{1})t}.$

 $P(SuccentExp] \le 2^{-k_0 t + \delta}$.

Piding $t=S+k_{\rm b},$ we derive a contradiction, since, with this value of t we have $\mathbb{P}[g_n^{tt}+1]\mathbb{E}^{-k_1\beta-k_1^2+\delta} < \Pr[\mathsf{SucceedExp}] \le 2^{-k_1\beta-k_1^2+\delta}.$

 $c_{\mathcal{S}}' := \Pr[\mathsf{FailuFind}(\mathcal{I}_n) \cup \mathsf{BiolQuery}]$

 $\begin{aligned} &= \mathbb{E}_{\gamma,0}[\varepsilon_{F,c,0}'] \\ &\leq \mathbb{E}_{\gamma,0}\left[\varepsilon_{F,\gamma,0} + \frac{S^{1}(S+k_1)}{p}\right] \end{aligned}$

attradiction comes from the assumption that $\epsilon_F > 4|g_{\rm s}^{\rm st} + 1|2^{-k_{\rm c}}$. Thus,

 $= c_F + \frac{N^2(S + k_1)}{s} \le \frac{4(q_1^m + 1)}{s} + \frac{N^2(S + k_1)}{s}.$

Note that at the end of such of the d concurious of A., we either learn th

 $\log \frac{p-l}{\log R + \log g_m + \log |Tabbe|} \ge \log \frac{p-|Tabbe|}{Rg_m|Tabbe|} \ge \log \frac{p-d(3g_m + N)}{Rdg_m(3g_m + N)}$ We further observe that $\log \frac{p-d(3p_0+N)}{d(3p_0)(n+N)} \ge 1$ for $d=|p/((2Rg_{nn}+1)(3g_{nn}+N)|)$. Thus, with this value of d, we have that this not profit becomes at least 1 lat for each of the d executions of A_{nn} . Hence, the total bitingth of the encoding is at

 $S + \log \binom{|G|}{p} + \sum_{i=0}^{p} \log(p-i) - d = \log \frac{|G|^{2}}{|G|^{2} - p|^{2}} + S - d$ $\leq \log \frac{|G|^2}{(|G| - p)^2} + S - \frac{p}{(186n + 1)(16n + N)} + 1$ $\leq \log \frac{|\Omega|^p}{(|\Omega| - p)^2} + S - \frac{p}{4H_{2n}(q_m + N)} + 1.$

If we choose $R = (1 + \log p)/r$, then all if executions all full with the probability of most r $(1-c)^R \le e^{-cR} \le 2^{-cR} \le 2^{-1-\log p} = \frac{1}{2p} \le \frac{N}{2p}$

sunding over the $\frac{\pi}{2}$ different executions of A_{pe} , the probability that the prostine fails in at most 1/2. With this value of R, the encoding length

 $\log \frac{|G|!}{(|G|-p)!} + S + 1 - \frac{cp}{6q_{ac}(q_{ac} + N)(\log p + 1)}$ Reminder of Theorem 8. Let H = (Rg, Sgn, Vh) be a key-profited Schnere signature scheme and $p > \mathbb{P}^n$ be a prime variate. Let $N \in \mathbb{N}$ be a parameter and (R_n^m, R_n^m) be a pair of generic adjustables within an enough $g_n r : \mathbb{Z}_p = G$ such that A_n^m makes at most g_n^m queries to the maximum works $\mathbb{N}: (0, 1)^n = (0, 1)^n$ and english as N-bit bind S_n^m , and S_n^m makes at most $g_n^m : g_n^m : g_n$

 $\Pr\left[\mathsf{SigFwgs}^{r,N}_{A^{(r)}_{k,m_{r-m},n}}(k) - 1\right] \le c_r \text{ with }$ $\varepsilon = \tilde{\mathcal{O}}\left(\frac{(1/\kappa_n^2 + N)(\kappa_n^2 + N)}{\mu}\right) + \frac{N(\kappa_n^2 + \kappa_n^2)}{\mu} \tilde{\kappa}_n^2 + \frac{\kappa_n^2(\kappa_n^2 + \kappa_n^2)}{\mu} + \frac{N(\kappa_n^2 + \kappa_n^2)}{\mu} + \frac{N(\kappa_n^2 + \kappa_n^2)}{\mu},$

54 J. Blocki and S. Lee

Similar to Theorem 7, if $q_1^{\rm sp} \ge 10N(1+2\log p)$ and $S \ge 10\log(8p)$, then $\Pr\left[\operatorname{SigFwap}_{A_{\operatorname{Sign}_{S$ $\leq \frac{16S(g_{k}^{m})^{2}\log p}{2} + \frac{N(g_{k}^{m}g_{k}^{m}-g_{k}^{m})g_{k}^{m}+g_{k}^{m})}{2} + \frac{S(g_{k}^{m}+1)}{2} + \frac{N^{2}(S+k_{k})}{2}$

which completes the proof. Rendador of Cision 6. $Pr[DesctProgramming] \le \frac{N_0 q^{\alpha}}{a^{\beta}}$.

attacker previously submitted a query of the form $\mathsf{H}[g_{ij}](I_i)$). Since pk_i and I_i are referred candons, we have $\mathsf{Pr}[R_{ij}] \leq q_i^{m}/p^{m}$. We now define the event $\mathsf{DetectPeoptemming} = \bigcup_{j \leq X_i \neq j_m} R_{i,j}$. Applying union bounds, we have

 $\Pr[\mathsf{DetecProgramming}] = \Pr[\bot_{i,j}B_{i,j}] \leq \sum_{i} \Pr[B_{i,j}] \leq \frac{N \frac{n}{2^{i}} S_{i}^{n}}{p^{i}}. \qquad \Box$

Roundandor of Claim 1. $\Pr[FultoFind(I_n).AbstQuery] \le \frac{d(g_n^n+1)}{g_n} + \frac{N^n(S+k_1)}{s}$. Proof of Claim 5: Fixing τ and H, and for some parameter t (which we will determine later), we define $\varepsilon_{F,\tau,0}$ to be

where the probability is taken over the random selection of $x_1, \dots, x_N \in \mathbb{Z}_q \setminus Y$ and the maximum costs of $A_{m_1, m_1, n_1}^{m_1}$. We can argue that remarking SY = SY points does not impact this probability, i.e., $x_{SY, n} = x_{SY, n$

(ii) For $i \in [\ell]$, sample $P = (x'_1, \dots, x'_N)$ subject to the contriction that $x'_j \neq x'_{j'}$ for any pair $(i,j) \neq (i',j')$.

(ii) Pots $i' \in [0,x_0^m]$ sufferency of random.

(ii) If q' = 0, then wait for the [interspired] found signature $a_i = (a_i,a_i)$ to be output, compute $L = r(a_i - a_ix_1^i)$, and suspen the prediction $H(r(x))(L(a_n) - a_n^i)$.

Lemma 4 has appeared in prior work in various forms. To the best of our knowledge, the original usage is from [00,Wal] though our statement is closer to a form from [00]Wall > 10, Since we rephrase the lemma slightly, we include a proof of Lemma 4 below for completeness.

Definition 4 (b-bit prediction game). Let B be a uniformly random let aring and let A be an algorithm that receives a kind $h = f(B) \in B$ which may depend arbitrarily on B and can additionally query B at specify indices higher adjusting indices h_1, \dots, h_k and bits h_1, \dots, h_k . We say that A wine the high prediction game of for all $j \le k$ we have $B[t_j] = b_j$ and A did not previously query for $B[t_j]$.

Lemma 4 ([DKW11,BHK $^{\circ}$ H]). Any attacker A wise the k-bit prediction gone with probability at most $|M/2^{\circ}$.

Poof. Let Success, denote the attacker's success probability when h=f(B) depends on E. Suppose for contradiction that $P(Success,g)>|H|2^{-k}$, then consider the algorithm A' which takes so bist, samples $h\in H$ uniformly, and simulates A with bint h. We have $\Pr[Success_{\mathcal{A}}] \ge \Pr[h = f(B)] \Pr[Success_{\mathcal{A}}] > \frac{1}{|M|} |H|T^{-1} = T^{-1}.$

To obtain a contradiction, we observe that A^i exceeds with probability at most 2^{-k} . In particolar, A^i starts with no hint and outputs i_1, \ldots, i_k and bits i_1, \ldots, i_k such the $B[i_j]$ has not been queried for all $j \leq k$. In this case, we can size such $B[i_j]$ are an informly random into sampled offer A^i outputs. Thus, $Pr[i_j] \leq k$, $b_j = B[i_j] = 2^{-k}$, which implies that $Pr[i_0 \cos m_i c_j] \leq 2^{-k}$.

Bandoder of Theorem 6. The Chaum-Polersen-FDH signature scheme is $\left(S, \phi_{N, D_{1}, D_{2}}, \theta_{1}, \theta_{2}^{-1}\right) \right)$ MU-UF-CMA source under the generic group model of prime order p is 2^{24} and the programmable random aracle model, where q denotes the total number of queries made by an adversary.

Food Shirth of Planess 2: Let H be the Chause-Podersen-FDH signature scheme. We follow a similar reduction as in Theorem 6 using the signing oracle without incovering at the secret lay x_i in Figure 3 (top). Note that the corresponding public key in $pk_j = \tau(x_i)$. Whenever the attacker species the random such of the form N(h(g)(x)) we can ensure that x_i a and b of appear in our b. C by using the reach Heigel (m, m) from the part. Letting c = H(h(g)(x)), we then compute $Pun(gh_{i,j})$ and $Luv(Pun(gh_{i,j},c))$ to ensure that both the topics $(Pun(gh_{i,j+1}), c_i, f_i)$ and $(Luv(Pun(gh_{i,j},c))$ to ensure that both the topics $(Pun(gh_{i,j+1}), c_i, f_i)$ and $(Luv(Pun(gh_{i,j+1}), c_i, f_i)$ and $(Luv(Pun(gh_{i,j+1}), c_i, f_i)$ because of W first consider the event W and W for consider the W

gh for practical attacks)



Summary of Our Results

Research Questions



Are short Schnorr signatures secure against preprocessing attacks?

Answer 3: Yes, "short" version of standardized implementations of Schnorr signatures are secure!