Fully Dynamic Attribute-Based Signatures for Circuits from Codes

S. Ling K. Nguyen D. H. Phan **K. H. Tang** H. Wang Y. Xu

16 April 2024

Outline

Attribute-Based Signatures

Stern Protocol

Our Contributions

Fully Dynamic Attribute-Based Signatures

Revisiting Stern

Our Results

Attribute-Based Signatures

Attribute-Based Signatures

Attribute-Based Signatures (ABS) [MPR11]:

- Each user has an independent attribute x.
- User can anonymous sign with public P if $P(x) = 1$.

Properties:

- *Correctness.*
- *Privacy.* Anonymous among attributes satisfying P.
- *Unforgeability.* Unable to forge signatures without valid signing keys.

Developments of ABS

Developments:

1. *Expanding expressiveness of signing policies.* Non-monotone access structures [OT11], bounded-depth circuits [Tsa17], unbounded arithmetic branching programs [DOT19], ...
2. *Functionalities.* traceability [EHM11], linkability [EG17], ...
3. *Computational assumptions.* pairing-based [MPR11], post-quantum [BK16], ...

Stern Protocol

Stern's Original Protocol

$\mathbf{w} \in \mathcal{B}_w^D$: length-$D$ binary vector of weight w.

Original Stern protocol [Ste96] addresses

$$\mathrm{R}_{\mathsf{stern}} = \left\{ \mathbf{M}, \mathbf{v};\ \mathbf{w} \;\middle|\; \mathbf{M} \in \mathbb{Z}_2^{D_0 \times D}, \mathbf{v} \in \mathbb{Z}_2^{D_0}, \mathbf{w} \in \mathcal{B}_w^D, \mathbf{M} \cdot \mathbf{w} = \mathbf{v} \right\}.$$

Stern's technique:

- Showing $\mathbf{M} \cdot \mathbf{w} = \mathbf{v}$: Use $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_2^D$ and set $\mathbf{z} := \mathbf{w} \oplus \mathbf{r}$.
  Then, show $\mathbf{M} \cdot \mathbf{z} = \mathbf{v} \oplus \mathbf{M} \cdot \mathbf{r}$.
- Showing $\mathrm{wt}(\mathbf{w}) = w$: Use $\phi \xleftarrow{\$} \mathcal{S}_D$.
  Then, show $\mathrm{wt}(\phi(\mathbf{w})) = w$.

Observations

Stern's technique:

- Showing $\mathbf{M} \cdot \mathbf{w} = \mathbf{v}$: Use $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_2^D$ and set $\mathbf{z} := \mathbf{w} \oplus \mathbf{r}$.
  Then, show $\mathbf{M} \cdot \mathbf{z} = \mathbf{v} \oplus \mathbf{M} \cdot \mathbf{r}$.
- Showing $\mathrm{wt}(\mathbf{w}) = w$: Use $\phi \xleftarrow{\$} \mathcal{S}_D$.
  Then, show $\mathrm{wt}(\phi(\mathbf{w})) = w$.

Initial Observations:

- $\mathbf{r}$ masks $\mathbf{w}$. Should $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_2^D$?
- ϕ hides $\mathbf{w}$ but keep weight. Should $\phi \xleftarrow{\$} \mathcal{S}_D$?

Our Contributions

Our Contributions

New Notion of ABS:

- *Full dynamicity (FDABS).* Dynamic enrollments, key updates, revocations.
- *Code-Based FDABS.* post-quantum assumptions, supporting arbitrary Boolean circuits, QROM-secure.

Revisiting Stern and Code-Based ZK:

- New general design capturing previous work from Stern.
  - Achieving efficiency by different view of masks and permutations.

Fully Dynamic Attribute-Based Signatures

FDABS

Challenge:

- Revocation does not allow users with revoked keys to sign.
- Require time-related update of system's public information.

Syntax: Follow framework of FDGS [BCC^{+}20].

- Maintain a registry reg for updating user keys.
- Update system information when updating reg.
- Each signature Σ is associated with epoch τ.
- Verifying Σ requires τ and system information.

Privacy: Anonymity is against maliciously generated keys.

Unforgeability: Unable to produce signatures with bad keys, not complying P or inactive users.

Designing Code-Based FDABS

Components: Merkle-tree (MT) accumulator [NTWZ19], commitment scheme [NTWZ19], and Stern-like ZKAoK [Ste96].

Design: Derive ideas from [NSS$^+$21, LNWX19].

- Commit to attributes at the leaves of MT, i.e., $\mathbf{d} = \mathrm{com}(\mathbf{x}, \mathbf{r})$.
- At each signing with policy P, show that
  - $\mathbf{d}$ belongs to the leaves,
  - $\mathbf{d}$ is valid commitment to $\mathbf{x}$, and
  - $P(\mathbf{x}) = 1$.
- Apply Unruh transform [Unr15, FLW19] for security in QROM.

ZKAoK for signing is revisited (next section).

Revisiting Stern

Observations

Initial Observations:

- $\mathbf{r}$ masks $\mathbf{w}$. Should $\mathbf{r} \overset{\$}{\leftarrow} \mathbb{Z}_2^D$? **No**.
- ϕ hides $\mathbf{w}$ but keep weight. Should $\phi \overset{\$}{\leftarrow} \mathcal{S}_D$? **No**.

Example: $\mathbf{w} \in \mathcal{B}^D_{\text{odd}}$ and $\mathbf{r} \overset{\$}{\leftarrow} \mathcal{B}^D_{\text{odd}} \Rightarrow \mathbf{w} \oplus \mathbf{r}$ is uniform in $\mathcal{B}^D_{\text{even}}$.

New Abstraction of Stern

Capturing Witness Set: $\mathbf{w} \in \mathrm{VALID}$.

Random Masks: $\mathbf{r} \xleftarrow{\$} \mathcal{R} \iff \mathbf{w} \oplus \mathbf{r}$ uniform in $\mathcal{Z}$.

Equivalently, $\left\{ \mathbf{z} = \mathbf{w} \oplus \mathbf{r} \;\middle|\; \mathbf{r} \xleftarrow{\$} \mathcal{R} \right\} \sim \left\{ \mathbf{z} \;\middle|\; \mathbf{z} \xleftarrow{\$} \mathcal{Z} \right\}$.

Random Functions for Proving $\mathbf{w} \in \mathrm{VALID}$: Define

- $\mathcal{S}$ to be a finite set,
- $F : \mathcal{S} \times \mathbb{Z}_2^D \to \mathbb{Z}_2^D$, $F' : \mathcal{S} \times \mathcal{R} \to \mathcal{R}$, $F'' : \mathcal{S} \times \mathcal{Z} \to \mathcal{Z}$.

Capture the following properties:

- $\forall \phi \in \mathcal{S} : F(\phi, \mathbf{w}) \in \mathrm{VALID} \iff \mathbf{w} \in \mathrm{VALID}$.
- $\phi \xleftarrow{\$} \mathcal{S} \iff F(\phi, \mathbf{w})$ uniform in VALID.
- *"Homomorphism".* $F'(\phi, \mathbf{r}) \oplus F''(\phi, \mathbf{z}) = F(\phi, \mathbf{r} \oplus \mathbf{z})$.

Proving NAND Gates

NAND gate: x_1 nand $x_2 = x_1 \cdot x_2 \oplus 1$.

Aim: Proving $x_3 = x_1$ nand x_2.

$\mathrm{ENC}(x_1, x_2, x_3) = (\overline{x_1} \cdot \overline{x_2} \oplus x_3, \overline{x_1} \cdot x_2 \oplus x_3, x_1 \cdot \overline{x_2} \oplus x_3, x_1 \cdot x_2 \oplus x_3)$.

$\mathrm{VALID} = \left\{ \mathrm{ENC}(x_1, x_2, x_3) \;\middle|\; x_1, x_2, x_3 \in \mathbb{Z}_2 \right\}$.

Observation:

$x_3 = x_1 \text{ nand } x_2 \iff \mathbf{w} = \mathrm{ENC}(x_1, x_2, x_3) \in \mathrm{VALID} \wedge \mathbf{w} = (\ldots, 1)$.

Proving NAND Gates (Continued)

Masks and Functions for Proving:

$\mathcal{S} = \mathbb{Z}_2^3$, $\mathcal{R} = \mathcal{B}_{\mathrm{odd}}^4$ and $\mathcal{Z} = \mathcal{B}_{\mathrm{even}}^4$.

$T((e_1, e_2), (y_{0,0}, y_{0,1}, y_{1,0}, y_{1,1})) = (y_{e_1,e_2}, y_{e_1,\overline{e_2}}, y_{\overline{e_1},e_2}, y_{\overline{e_1},\overline{e_2}})$.

$F : \mathcal{S} \times \mathbb{Z}_2^4 \to \mathbb{Z}_2^4 :: ((e_1, e_2, e_3), \mathbf{y}) \mapsto T((e_1, e_2), \mathbf{y}) \oplus (e_3, e_3, e_3, e_3)$.
$F' : \mathcal{S} \times \mathcal{R} \to \mathcal{R} :: ((e_1, e_2, e_3), \mathbf{y}) \mapsto T((e_1, e_2), \mathbf{y})$.
$F'' : \mathcal{S} \times \mathcal{Z} \to \mathcal{Z} :: ((e_1, e_2, e_3), \mathbf{y}) \mapsto T((e_1, e_2), \mathbf{y}) \oplus (e_3, e_3, e_3, e_3)$.

Our Results

Scheme	Policy expressiveness	Assumptions	SM/ (Q)ROM	Signature size	Fully dynamic
[OT11]	Non-monotone access structures	pairings	SM	$\mathcal{O}(S \cdot \lambda)$	✗
[SAH16]	Arbitrary circuits	pairings	SM	$\mathcal{O}(C \cdot \lambda)$	✗
[SKAH18]-1	Turing machines	pairings	SM	$\mathcal{O}(T^2 \cdot \lambda)$	✗
[SKAH18]-2	Non-deterministic finite automata	pairings	SM	$\mathcal{O}(W \cdot \lambda)$	✗
[DOT19]	Branching programs	pairings	SM	$\mathcal{O}(L \cdot \lambda)$	✗
[Tsa17]	Bounded-depth circuits	lattices	SM	$\widetilde{\mathcal{O}}(D \cdot \lambda)$	✗
[EK18]	Arbitrary circuits	lattices	ROM	$\widetilde{\mathcal{O}}(C \cdot \lambda^2 + \lambda^3)$	✗
Ours	Arbitrary circuits	codes	QROM	$\widetilde{\mathcal{O}}(C \cdot \lambda + \lambda^2)$	✓

Thank You!

[BCC+20] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, and Jens Groth.
Foundations of fully dynamic group signatures.
J. Cryptol., 2020.

[BK16] Rachid El Bansarkhani and Ali El Kaafarani.
Post-quantum attribute-based signatures from lattice assumptions.
Cryptology ePrint Archive, Paper 2016/823, 2016.
`https://eprint.iacr.org/2016/823`.

[DOT19] Pratish Datta, Tatsuaki Okamoto, and Katsuyuki Takashima.
Efficient attribute-based signatures for unbounded arithmetic branching programs.
In *PKC 2019*, 2019.

[EG17] Ali El Kaafarani and Essam Ghadafi.
Attribute-based signatures with user-controlled linkability without random oracles.
In Máire O'Neill, editor, *IMACC 2017*, 2017.

[EHM11] Alex Escala, Javier Herranz, and Paz Morillo.
Revocable attribute-based signatures with adaptive security in the standard model.
In *AFRICACRYPT 2011*, 2011.

[EK18] Ali El Kaafarani and Shuichi Katsumata.
Attribute-based signatures for unbounded circuits in the ROM and efficient instantiations from lattices.
In *PKC 2018*, 2018.

[FLW19] Hanwen Feng, Jianwei Liu, and Qianhong Wu.
Secure stern signatures in quantum random oracle model.
In *ISC 2019*, 2019.

[LNWX19] San Ling, Khoa Nguyen, Huaxiong Wang, and Yanhong Xu.
Lattice-based group signatures: Achieving full dynamicity (and deniability) with ease.
Theor. Comput. Sci., 2019.

[MPR11] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek.
Attribute-based signatures.
In *CT-RSA 2011*, 2011.

[NSS+21] Khoa Nguyen, Reihaneh Safavi-Naini, Willy Susilo, Huaxiong Wang, Yanhong Xu, and Neng Zeng.
Group encryption: Full dynamicity, message filtering and code-based instantiation.
In *PKC 2021*, 2021.

[NTWZ19] Khoa Nguyen, Hanh Tang, Huaxiong Wang, and Neng Zeng.
New code-based privacy-preserving cryptographic constructions.
In *ASIACRYPT 2019*, 2019.

[OT11] Tatsuaki Okamoto and Katsuyuki Takashima.
Efficient attribute-based signatures for non-monotone predicates in the standard model.
In *PKC 2011*, 2011.

[SAH16] Yusuke Sakai, Nuttapong Attrapadung, and Goichiro Hanaoka.
Attribute-based signatures for circuits from bilinear map.
In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *PKC 2016*, 2016.

[SKAH18] Yusuke Sakai, Shuichi Katsumata, Nuttapong Attrapadung, and Goichiro Hanaoka.
Attribute-based signatures for unbounded languages from standard assumptions.
In *ASIACRYPT 2018*, 2018.

[Ste96] Jacques Stern.
A new paradigm for public key identification.
IEEE Trans. Inf. Theory, 1996.

[Tsa17] Rotem Tsabary.
An equivalence between attribute-based signatures and homomorphic signatures, and new constructions for both.
In *TCC 2017*, 2017.

[Unr15] Dominique Unruh.
Non-interactive zero-knowledge proofs in the quantum random oracle model.
In *EUROCRYPT 2015*, 2015.