A Tale of BBS Credentials

PRIVCRYPT 2026
Rome, May 2026

PAUL G. ALLEN SCHOOL
OF COMPUTER SCIENCE & ENGINEERING

Stefano Tessaro

tessaro@cs.washington.edu

Digital Credentials

X.509, RFC 5755 X.509, OpenID Connect, SAML 2.0, W3C Verifiable Credentials (VC / JWT-VC), ISO/IEC (mDL), eIDAS, …

= signature on credential with sk_{Iss}

Issuer

sk_{Iss}

Name:	Jane Doe
Address:	1234, 1st Ave
City:	Seattle
State:	WA
Zip:	98101
DoB:	1/1/2000
User key:	pk_U

User

Name:	Jane Doe
Address:	1234, 1st Ave
City:	Seattle
State:	WA
Zip:	98101
DoB:	1/1/2000
User key:	pk_U

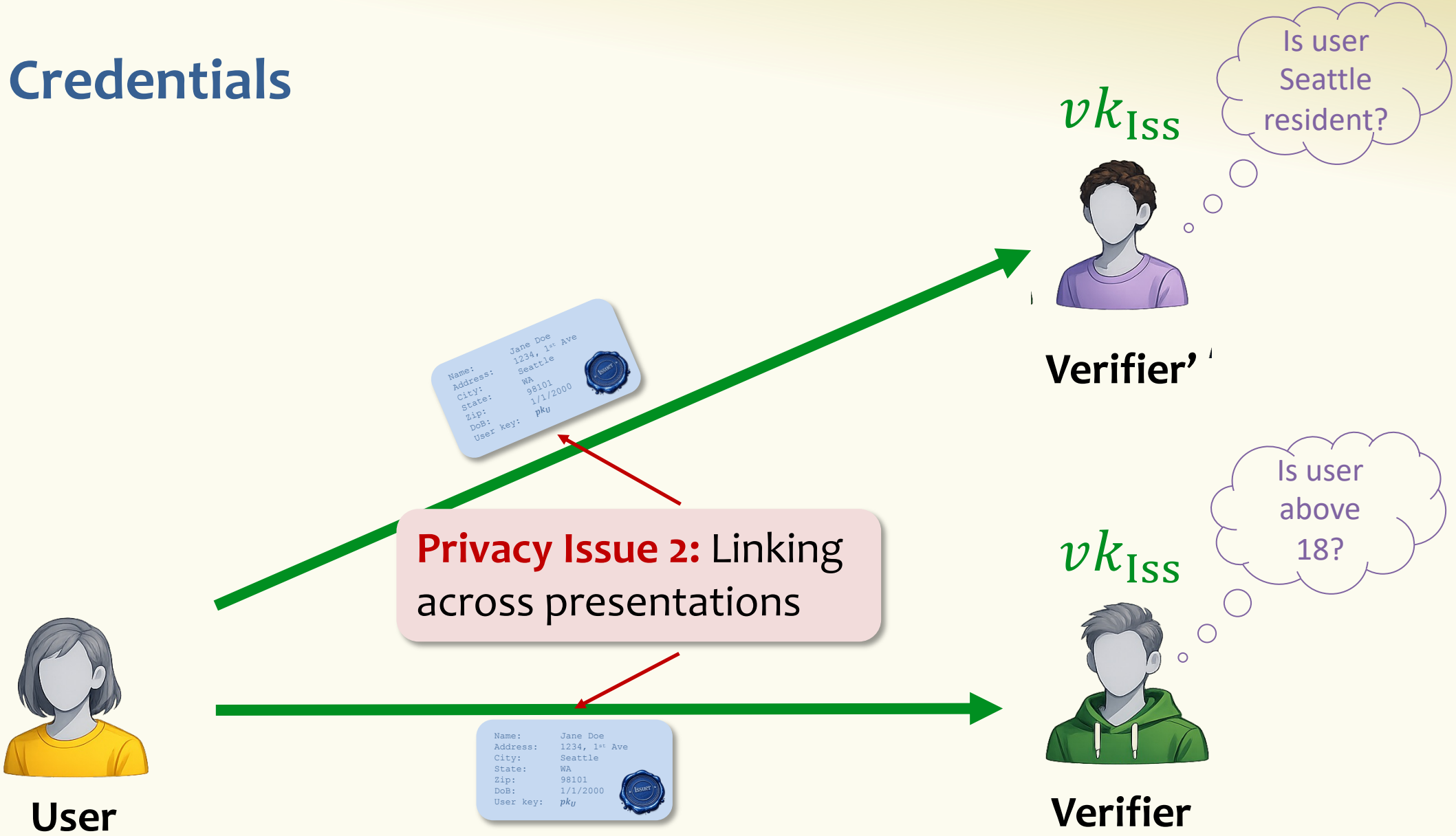
vk_{Iss}

Is user above 18?

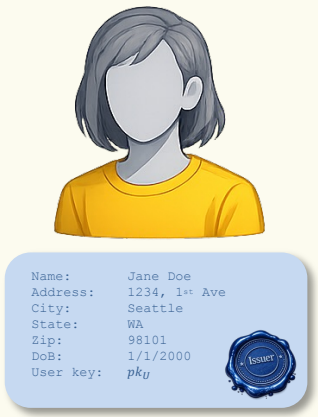
Verifier

Privacy Issue 1:
Reveals <u>all</u> attributes

Digital Credentials



Anonymous Credentials (ACs) [Chaum '84; Camenisch-Lysyanskaya '01]



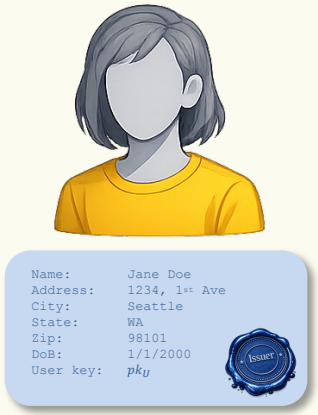
$\pi = \text{ZKProof}$ [*"I have a valid credential attesting that my age >=18"*]

Minimal disclosure + unlinkability

W3C Verifiable Credentials, Decentralized Identity Foundation (DIF), Hyperledger Indy / Aries (AnonCreds), ISO/IEC 18013-5 mDL, SD-JWT, eIDAS 2.0 / EU Digital Identity Wallet, Idemix (IBM), U-Prove (Microsoft), Google (Longfellow), …

Gained significant momentum due to recent interest from governments (e.g., EUDI Wallet)

Anonymous Credentials (ACs) [Chaum '84; Camenisch-Lysyanskaya '01]



$\pi = \text{ZKProof}$ [*"I have a valid credential attesting that my age >=18"*]

Minimal disclosure + unlinkability

vk_{Iss}

Is user above 18?

Generic ZK proofs supporting any credential format

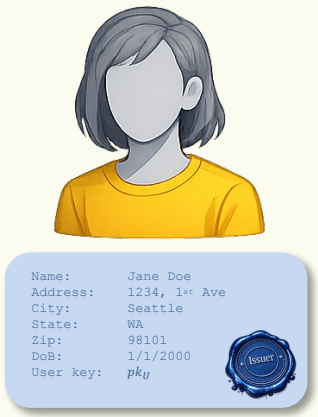
Example: Google Longfellow
Flexible, but slow & complex

VS

Tailor-made digital signatures with efficient ZKPs

Example: CL, BBS, PS, …
Lightweight, less flexible

Anonymous Credentials (ACs)



$\pi = \text{ZKProof}$ [*"I have a valid credential attesting that my age >=18"*]

Minimal disclosure + unlinkability

Generic ZK proofs supporting any credential format

VS

Tailor-made digital signatures with efficient ZKPs

Example: Google Longfellow
Flexible, but slow & complex

Example: CL, BBS, PS, …
Lightweight, less flexible

BBS – Standardization

CFRG/IRTF

- BBS-Signatures (draft-irtf-cfrg-bbs-signatures)
- BBS per Verifier Linkability (draft-irtf-cfrg-bbs-per-verifier-linkability)
- Blind BBS Signatures (draft-irtf-cfrg-bbs-blind-signatures)

ISO

- Anonymous Digital Signatures (ISO/IEC 20008-2:2013)
- Attribute-based Credentials (ISO/IEC 24843)

IETF PrivacyPass

- Anonymous Credit Tokens (draft-schlesinger-cfrg-act, BBS-MAC)

ETSI

- ZKP-EUDI-Wallet (BBS/ECDSA-Variant, ETSI TS 119 476-2 Work plan)

W3C

- Data Integrity BBS Cryptosuites v1.0

(Thanks to Anja Lehmann for pointing out many of these!)

This talk, in a nutshell

What BBS signatures can and cannot do

History of BBS/BBS+

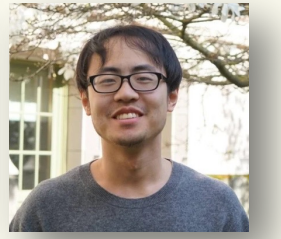
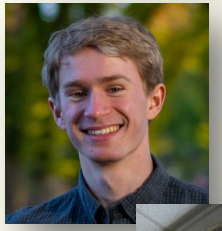
Analysis of BBS & standardization impact

① Revisiting BBS Signatures
[w/ C. Zhu @ EUROCRYPT '23]

② Server-Aided Anonymous Credentials
[w/ R. Chairattana-Apirom, F. Harding, and A. Lysyanskaya @ CRYPTO '25]

③ On the Concrete Security of BBS/BBS+ Signatures
[w/ R. Chairattana-Apirom @ ASIACRYPT '25]

④ Tight Security for BBS Signatures
[w/ R. Chairattana-Apirom and D. Hofheinz @ EUROCRYPT '26]

Disclaimers

- **Not post-quantum secure**
  - However: many protocols built on top of BBS achieve unconditional (and thus post-quantum) privacy!
- **Pairing-based**
  - But also: Reasonable deployment scenarios w/o pairings
- **Undesirable features:** Expensive threshold, difficult device binding, no re-randomization, etc.

This talk (and surrounding research): Neutral take, study of object of interest – (my) goal is not to declare a winner!

Part I: Definition & History

BBS Signatures [Boneh-Boyen-Shacham '04, Camenisch-Lysyanskaya '04]

$G, H_1, \ldots, H_\ell$ = distinct generator of $\mathbb{G}_1$, prime order p

Signing key: $sk \in \mathbb{Z}_p$ Verification key: $VK = skG_2 \in \mathbb{G}_2$

Attributes: $a_1, \ldots, a_\ell \in \mathbb{Z}_p$

$$\sigma(sk, (a_1 \ldots . a_\ell)) = \left(\underbrace{\frac{G + a_1H_1 + a_2H_2 + \cdots + a_\ell H_\ell}{sk - e}}_{48B}, \underbrace{e}_{32B}\right), e \leftarrow \mathbb{Z}_p$$

$\sigma = (A, e)$ valid for $a_1, \ldots, a_\ell$ iff

Minor pet peeve: Original scheme uses +, not -

$$\mathrm{e}(A, VK - eG_2) = \mathrm{e}(G + a_1H_1 + a_2H_2 + \cdots + a_\ell H_\ell, G_2)$$

BBS Signatures – Selective Disclosure

Statement = VK, i, a^*

"*I know a valid* $\sigma = (A, e)$ *for* VK on $\vec{a} = (a_1, \ldots, a_\ell)$ s.t. $a_i = a^*$"

Randomization: $\bar{A} = rA, \bar{B} = r(G + \sum_i a_i H_i + eA), r \leftarrow \mathbb{Z}_p^*$

$sk\bar{A} = \bar{B}$

$$G + a^* H_i = r^{-1}\bar{B} - r^{-1}e\bar{A} - \sum_{j \neq i} a_j H_j$$

Proof = $\bar{A}, \bar{B}$ + PoK of $\alpha, \beta, (\delta_j)_{j \neq i}$ s.t. $G + a^* H_i = \alpha\bar{B} + \beta\bar{A} + \sum_{j \neq i} \delta_j H_j$

Many alternatives: [Camenisch-Drijvers-Lehmann '16] [**T**-Zhu '23] [Whitehead '24]

BBS Signatures – Pseudonyms

Statement = VK, nonce, nym

"I know a valid $\sigma = (A, e)$ *for* VK on $\vec{a} = (a_1, \ldots, a_\ell)$ *such that* $a_1 = k$ *and* $\text{nym} = k \cdot H(\text{nonce})$*"*

DDH-based PRF

Proof = $\bar{A}, \bar{B}$ + PoK of $\alpha, \beta, (\delta_j)_i$ s.t. $G = \alpha\bar{B} + \beta\bar{A} + \sum_i \delta_j H_j$ and $\text{nym} = \delta_1 \cdot H(\text{nonce})$

Framework easily extends to pretty much everything provable via Schnorr type proofs

BBS Signatures – Blind Issuance

Issuer

sk

$\rho \leftarrow \mathbb{Z}_p$

$\mathrm{COM} = \rho H_0 + a_1 H_1 + a_2 H_2 + \cdots + a_\ell H_\ell$

+ consistency proof

$\sigma = \left(A = \frac{G + \mathrm{COM}}{sk - e}, e\right)$

Not a blind signature!

User

[Orrù CCS '25] multiplicative blinding ⟹ more efficient presentation proofs

[ChatGPT Prompt: “humorously illustrate going down the rabbit hole of BBS history”]

BBS History

No proof of security in either paper

Look, it's BBS!

Our group signature scheme can be extended to provide strong exculpability using a similar mechanism. Instead of simply giving user i the private key $(g_1^{1/(\gamma+x_i)}, x_i)$, the user and key issuer engage in a JOIN protocol where at the end of the protocol user i has a triple (A_i, x_i, y_i) such that $A_i^{\gamma+x_i} h_1^{y_i} = g_1$ for some public parameter h_1. The value y_i is chosen by the user and is kept secret from the key issuer. The ZKPK of Section 4 can be modified to prove knowledge of such a triple. The resulting system is a short group signature with strong exculpability.

[Boneh-Boyen-Shacham CRYPTO '04]

Not surprisingly, this signature scheme can be extended to the equivalent of our Schemes B and C using techniques similar to the ones described above. As a result, we can obtain signature schemes with efficient protocols based on the BBS signature. Let us give a sketch for the equivalent for Scheme C. A public key would be $(g_1, g_2, h_0, h_1, \ldots, h_\ell)$. A signature on a block of messages $(m_0, \ldots, m_\ell)$ consists of values (A, x) such that $A^{\gamma+x} \prod_{i=0}^{\ell} h_i^{m_i}$. In order to obtain a signature on a committed block of messages, a user will have to supply the signer with the value $Y = \prod_{i=0}^{\ell} h_i^{m_i}$, and prove knowledge of its representation in the bases $(h_0, \ldots, h_\ell)$. If m_0 is chosen at random, then Y information-theoretically hides $(m_1, \ldots, m_\ell)$. The signer will then generate the signature. A proof of knowledge of a signature on a committed value can be obtained by appropriate modifications to the BBS group signature protocol.

[Camenisch-Lysyanskaya CRYPTO '04]

Look, it's BBS! (but forgot "$= g_1$")

BBS+

$$\sigma(sk, (a_1 \ldots . a_\ell)) = \left(\frac{G + sH_0 + a_1H_1 + a_2H_2 + \cdots + a_\ell H_\ell}{sk - e}, s, e\right), s, e \leftarrow \mathbb{Z}_p$$

Constant-Size Dynamic *k*-TAA* **

Man Ho Au[1], Willy Susilo[1], and Yi Mu[1]

Center for Information Security Research
School of Information Technology and Computer Science
University of Wollongong, Wollongong 2522, Australia
{mhaa456,wsusilo,ymu}@uow.edu.au

$$\mathrm{Adv}^{\text{suf-cma}}_{\text{BBS+}}(t, q) \leq q \cdot \mathrm{Adv}^{q\text{-sdh}}_{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T}(t')$$

q = # issued signatures

[Au-Susilo-Mu SCN '06] [Au-Susilo-Mu-Chow IEEE Syst. J '13]

Extended to Type III pairings [Camenisch-Drijvers-Lehmann TRUST '16]

q-SDH: $G, xG, x^2G, \ldots, x^qG, G_2, xG_2 \Longrightarrow^? \left(e, \frac{1}{x+e}G\right)$ [Boneh-Boyen '04+'08]

[Okamoto TCC '06] Special case $\ell = 1$

More relevant works

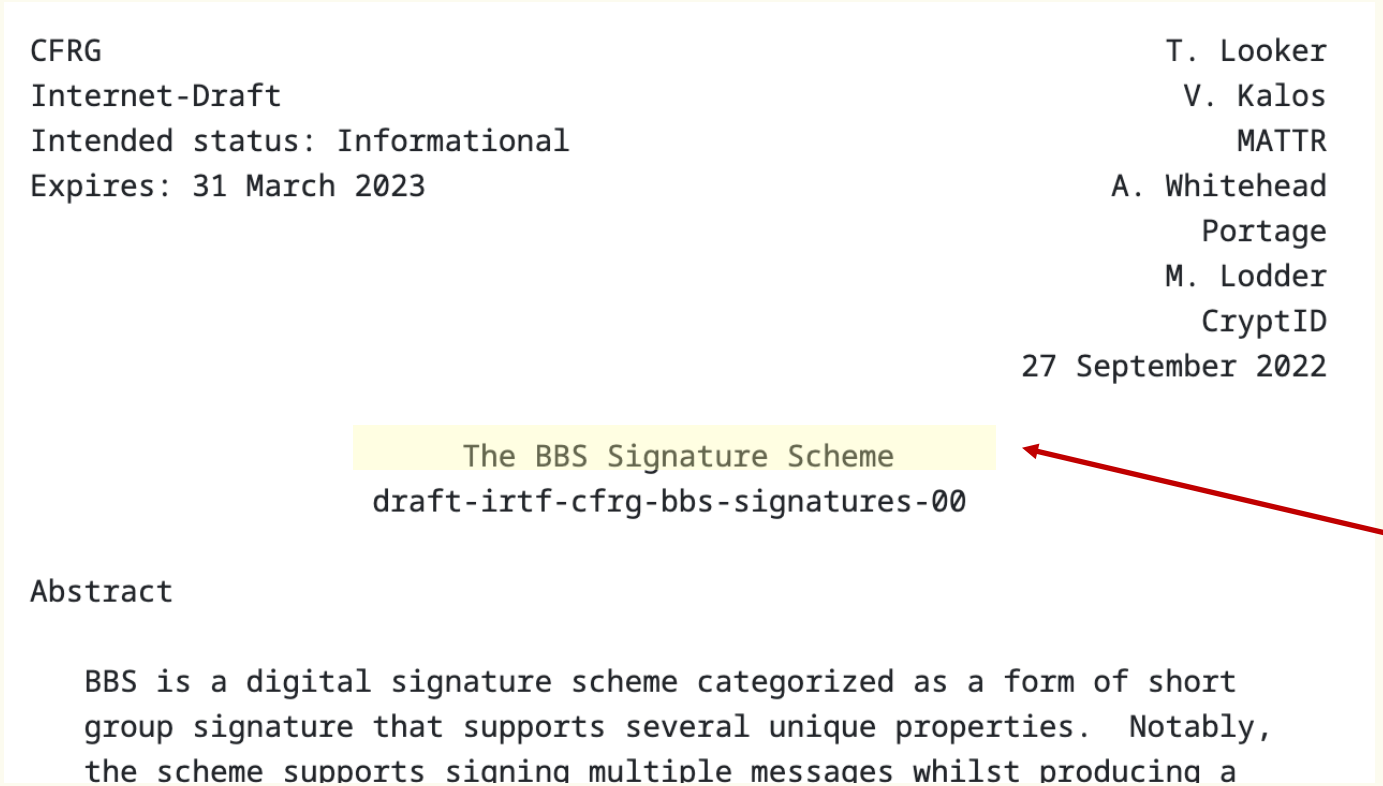
- **Non-tight** security proof for BBS with **bit** attributes under q-SDH
  [Hofheinz-Kiltz CRYPTO '08]
- **Tight** reduction from q-SDH for BBS+
  [Schäge EUROCRYPT '11]
- Incorrect proof of security for BBS
  [Chen Inscrypt '09] [Brickell-Li TRUST '10]

Did not know about BBS line of work

Most of this work was on DAA (aka ACs in disguise)

Part II: Our work

2022: Standardization efforts for BBS+ underway



CFRG
Internet-Draft
Intended status: Informational
Expires: 31 March 2023

T. Looker
V. Kalos
MATTR
A. Whitehead
Portage
M. Lodder
CryptID

27 September 2022

The BBS Signature Scheme
draft-irtf-cfrg-bbs-signatures-00

Abstract

BBS is a digital signature scheme categorized as a form of short group signature that supports several unique properties. Notably, the scheme supports signing multiple messages whilst producing a

Confusingly, they meant BBS+!

Major Seattle-area tech company asks us a few questions about BBS+ security proofs.

Us: Do we need BBS+? Can we prove BBS also secure?

Do we need BBS+? Can we prove BBS also secure?

$$\mathrm{Adv}^{\mathrm{suf-cma}}_{\mathrm{BBS}}(t,q) \leq q \cdot \mathrm{Adv}^{q-\mathrm{sdh}}_{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T}(t')$$

Standard model

Think: $t' \approx t$

$$\mathrm{Adv}^{\mathrm{suf-cma}}_{\mathrm{BBS}}(t,q) \leq \mathrm{Adv}^{q-\mathrm{sdh}}_{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T}(t')$$

AGM

[**T**-Zhu EUROCRYPT '23]

Immediate reaction: RFC standardization turned from BBS+ to BBS

Issue 1: Tightness

$$\mathrm{Adv}^{\mathrm{suf-cma}}_{\mathrm{BBS}}(t,q) \le q \cdot \mathrm{Adv}^{q-\mathrm{sdh}}_{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T}(t)$$

(GGM bound) $$\le q \cdot \frac{qt^2}{p} = \frac{(qt)^2}{p}$$

Tight by Cheon's attack [Cheon '06]: Break q-DL/q-SDH using $\sqrt{p/q}$ scalar multiplications and recovers secret key (for $q|(p-1)$)

BLS12-381: $p \approx 2^{256}, q = 2^{48} \rightarrow$ 80-bit security 😢

For BLS12-381: $p - 1 = 2^{32} \cdot 3 \cdot 11 \cdot 19 \cdot 10177 \cdot 125527 \cdot 859267 \cdot 906349^2 \cdot 2508409 \cdot 2529403 \cdot 52437899 \cdot 254760293^2$.

$$\mathrm{Adv}^{\mathrm{suf-cma}}_{\mathrm{BBS}}(t,q) \le \mathrm{Adv}^{q-\mathrm{sdh}}_{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T}(t) \le \frac{qt^2}{p}$$

BLS12-381: $p \approx 2^{256}, q = 2^{48} \rightarrow$ 104-bit security 🎉

[Note: Best-possible security is 120-bit due to DL in $\mathbb{G}_T$]

Issue 1: Tightness

Initially, lack of tight reduction was not an issue because only known reduction for BBS+ was equally not tight …

Unfortunately: Community missed tight BBS+ proof [Schäge EUROCRYPT ’11] – could BBS+ actually be more secure? 😬

Can we give a tight standard model reduction for BBS?

Issue 2: Cryptanalysis

① Sign a multiple times:

$$\frac{C}{x-e_1}, \frac{C}{x-e_2}, \ldots, \frac{C}{x-e_q}$$

$$C = G + aH$$

② Efficiently compute $x^i \hat{G}$ for $i = 0,1,\ldots,q$, for $\hat{G} = \frac{C}{\prod_{i=1}^{q}(x-e_i)}$

[Jao-Yoshida Pairing '09]

③ Compute q-DL to base $\hat{G}$

Cheon's attack [Cheon '06]: Break q-DL using $\sqrt{p/q}$ scalar multiplications and recovers secret key (for $q|(p-1)$)

However: Does not work with BBS+ and **deterministic** BBS

Can it be that deterministic BBS/BBS+ are <u>more</u> secure than q-DL / q-SDH?

Concrete Security – Two questions

Can we give a tight standard model reduction for BBS?

Yes, for deterministic BBS
No, for general plain BBS

[ChairattanaApirom-Hofheinz-**T** EUROCRYPT ’26]

Can it be that deterministic BBS/BBS+ are more secure than q-DL / q-SDH?

No

[ChairattanaApirom-**T** ASIACRYPT ’25]

[ChairattanaApirom-**T** ASIACRYPT '25]

Our Results – Attacks

Theorem. Let $d|(p-1)$. Then, $\exists \mathcal{A}_1$ making $q = 2d + 2$ distinct signing queries and $\sqrt{p/q}$ scalar multiplications such that

$$\mathrm{Adv}_{\mathrm{BBS}}^{\mathrm{suf-cma}}(\mathcal{A}_1) \geq 1 - \frac{1}{p}$$

Extensions:

- Similar attack applies to BBS+
- Can actually show: BBS/BBS+ security $\Longrightarrow$ hardness of q-SDH/q-DL

Our Results – Tigthness

[ChairattanaApirom-Hofheinz-**T** EUROCRYPT '26]

Theorem. For every time t adversary $\mathcal{A}$ making q distinct signing queries, there exists time t' adversary $\mathcal{B}$ such that

$$\mathrm{Adv}^{\mathrm{suf-cma}}_{\mathrm{BBS}}(t,q) \leq \Theta(1) \cdot \mathrm{Adv}^{d-\mathrm{sdh}}_{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T}(t') + \mathrm{negl}(\lambda)$$

$$d \approx 10q \qquad t' = t + O(q^2) \cdot \mathrm{poly}(\lambda)$$

Theorem. There exists (inefficient) SUF adversary $\mathcal{A}$ making q identical signing queries such that *for any* *algebraic reduction* $\mathcal{B}$ breaking d-SDH,

$$\mathrm{Adv}^{d-\mathrm{sdh}}_{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T}\left(\mathcal{B}^{\mathcal{A}}\right) \leq \Theta(q^{-1}) \cdot \mathrm{Adv}^{\mathrm{suf-cma}}_{\mathrm{BBS}}(\mathcal{A}) + \mathrm{negl}(\lambda)$$

Strong Unforgeability of BBS

Case 1: $e^* \notin \{e_i\}_i$.
Case 2: $\exists i^* \in [q]: e^* = e_{i^*}$.

Adversary $\mathcal{A}$

VK

$\vec{a}_i \in \mathbb{Z}_p^\ell$

(e_i, A_i)

$\left(\vec{a}^*, (e^*, A^*)\right)$

Hard part of the proof is **Case 2**

Main challenge captured by "game" involving polynomials

Polynomial Game

Pick degree-d $f(X), g(X)$ mod p

$m_i \neq 0$

$q\times$

e_i

① e_i uniform and independent of everything so far

② $f(e_i) + m_i g(e_i) = 0$

$i^* \in \{1, \dots, q\}$

Alice wins if $g(e_{i^*}) \neq 0$

Goal: $\min \Pr[win] \approx \text{const.} \;\&\; d = O(q)$

Polynomial Game

"Good" bad idea : $f(X) = g(X) = \prod_{i=1}^{q}(X - \delta_i)$ for $\delta_1, \ldots, \delta_q \leftarrow \mathbb{Z}_p$

$e_i = \delta_i$ uniform 👍 $\quad f(e_i) + m_i g(e_i) = 0$ for every m_i 👍

$g(e_{i^*}) = 0$ for every $i^* \in \{1,,,.q\}$ 👎

$$f(X) + mg(X) = f(X)(mX - m\delta_k + 1)$$

q roots: $\{\delta_i\}_{i \neq k} + \left(\delta_k - \frac{1}{m}\right)$

[T-Zhu '23] Pick $k \leftarrow [q], \delta_1, \ldots, \delta_q \leftarrow \mathbb{Z}_p$

$$\Pr[\text{win}] = 1/q$$

$$f(X) = \prod_{i \neq k}(X - \delta_i) \qquad g(X) = (X - \delta_k) f(X)$$

If $i^* = k$, then $e_{i^*} = \delta_k - \frac{1}{m_k}$ not a root of $g(X)$

$$e_i = \begin{cases} \delta_i, & i \neq k \\ \delta_k - \frac{1}{m_k}, & i = k \end{cases}$$ uniform 👍

Polynomial Game – Our strategy

Idea: Let

$$f(X) = \varphi(X)\prod_{i=1}^{q}(X-\delta_i) \qquad g(X) = -\beta\prod_{i=1}^{q}(X-\delta_i)$$

where $\delta_1, \dots, \delta_q, \beta \leftarrow \mathbb{Z}_p$ and $\varphi(X)$ random polynomial of degree $d = O(q)$

If $\varphi(X) - m_i\beta$ has a single zero e, set $e_i = e$, else $e_i = \delta_i$

Alice wins if $e_{i^*} \notin \{\delta_1, \dots, \delta_q\}$

We show: $\Pr[\text{win}] = \Omega(1)$

Our Analysis

Alice wins if $i^* \in S = \{i \in [q] : \exists!\, e \in \mathbb{Z}_p : \varphi(e) = m_i\beta\}$.

Core argument: Study joint distribution $\left((e_i)_{i\in[q]}, S\right)$

- **Lemma 1.** $(e_i)_{i\in[q]}$ are close to uniform and independent of S.
- **Lemma 2.** For any i^*, $\Pr[i^* \in S] \geq \frac{1}{e}$.

Tools: H-coefficient technique [Patarin'08] & $\Theta(q)$-wise independence of φ

Deterministic BBS

$$\sigma(sk, (a_1 \ldots . a_\ell)) = \left(\frac{G + a_1 H_1 + a_2 H_2 + \cdots + a_\ell H_\ell}{sk - e}, e\right)$$

Signing each message at most once = <u>derandomized</u> BBS

Option A: $e = \mathrm{PRF}(sk', (a_1, \ldots, a_\ell))$

→ BBS RFC draft

→ Not compatible with Blind Issuance RFC

Option B: $e = \mathrm{PRF}(sk', G + a_1 H_1 + a_2 H_2 + \cdots + a_\ell H_\ell)$

→ Compatible with additive Blind Issuance

Part III: Challenges & Alternatives

Challenges with BBS – Threshold, Aggregation, Re-randomization

Sad truth: $\frac{1}{sk_1 - e_1} + \frac{1}{sk_2 - e_2} \neq \frac{1}{sk_1 + sk_2 - e}$ for some $e = e(e_1, e_2)$

Still: **Several threshold protocols for BBS/BBS+** [caveat: #rounds ≥ 2]

[Doerner-Kondi-Lee-Shelat-Tyner IEEE S&P '23]
[Faust-Hazay-Kretzler-Rometsch-Schlosser CT-RSA '25]
[Tang-Qiu-Jiang-Xue-Yang-Au-Deng-Lam IEEE S&P '26]
[Wu-Qiu-Tang-Niu-Jiang-Zhou-Xue-Yang ESORICS '26] [Heng-Liu-Lu-Xue-Bao-Au PKC '26] …

Similar: No aggregation, no re-randomization, …

Challenges with BBS – Pairings

Use of pairings can be problematic

- **Device binding** (e.g., EUDI)
  - secure element issues signature in pairing-free curve, hard binding with credentials (see Anja's talk)
- **Lack of proper standardization**

BBS/BBS+ without pairings is an algebraic MAC

Pairing-free BBS – Use cases

- **Keyed-Verification Anonymous Credentials (KVAC)**
  [Barki-Brunet-Desmoulins-Traoré SCN ‘16] [Orrù CCS ‘25]
  - Issuer = verifier
- **Server-Aided Anonymous Credentials (SAAC)**
  [Desmoulins-Dumanois-Kane-Traoré ePrint ’25 BBS#] [ChairattanaApirom-Harding-Lysyanskaya-T CRYPTO ‘26]
  - Public-verifiability with helper

Proof = $\bar{A}, \bar{B}$ + PoK —— $sk\bar{A} = \bar{B}$ → Can be verified directly (KVAC)

$sk\bar{A} = \bar{B}$ → Can be verified with help of additional DLEQ proof (SAAC)

SAACs

[Desmoulins-Dumanois-Kane-Traoré ePrint '25 BBS#]
[ChairattanaApirom-Harding-Lysyanskaya-T CRYPTO '26]

$\sigma = (A, e) =$ credential

① $\bar{A}, \bar{B}$

③ $\pi = \bar{A}, \bar{B} + \pi_{DLEQ} +$ PoK

$VK = skG$

Is user above 18?

② Generate DLEQ proof π_{DLEQ} **obliviously**
[Orrù-T-Zaverucha-Zhu CRYPTO '24]

Issuer

sk

Possible Alternatives

Common take: *Why are they even using BBS?! There is a much better solution!!!*

My take: No clear winner! (And can see why BBS is preferred)

Possible Alternatives

Pairing-based signatures with efficient protocols

Scheme	Assumption	Concrete security	Key size	Sig size	Threshold / aggreg / rerand.
BBS	q-SDH	$\sqrt{p/q}$	$1\ \mathbb{Z}_p$ (sk) $1\ \mathbb{G}_2$ (vk)	$1\ \mathbb{G}_1 + 1\ \mathbb{Z}_p$	Not easy
PS	Ad-hoc q-type	$\sqrt{p}$	$\ell + 1\ \mathbb{Z}_p$ (sk) $\ell + 1\ \mathbb{G}_2$ (vk)	$2\ \mathbb{G}_1$	Easy
FRW	(2,1)-DL (AGM)	$\sqrt{p}$	$1\ \mathbb{G}_1 + 1\ \mathbb{Z}_p$ (sk) $2\ell + 2\ \mathbb{G}_1 + \ell + 2\ \mathbb{G}_2 +$ $1\mathbb{G}_T$ (vk)	$2\ \mathbb{G}_1$	Easy
SPS-EQ	GGM	$\sqrt{p/q}$	$\ell\ \mathbb{Z}_p$(sk) $\ell\ \mathbb{G}_2$ (vk)	$2\ \mathbb{G}_1 + 1\ \mathbb{G}_2$	Easy

+ constant-size presentation proofs

PS = Pointcheval, Sanders. Short Randomizable Signatures. CT-RSA 2016

FRW = Fuchsbauer, Regen, Wee. Round-Optimal Threshold Blind Signatures without Random Oracles. CRYPTO 2026

SPS-EQ = Fuchsbauer, Hanser, Slamanig. Structure-Preserving Signatures on Equivalence Classes and Constant-Size Anonymous Credentials. JoC 2019

Conclusions

- **BBS has attracted substantial interest**
  - Covered by multiple standards
  - Good object of study
- **We understand its concrete security pretty well**
  - Tightly connected to q-DL / q-SDH
  - No clear reason to use BBS+ over BBS (except for confusion)
- **No other solution strictly dominates BBS**

Thank you!