BBS+ Applications, Standardization, and a Bit of Theory

Dr. Greg Bernstein[1]

Vasilis Kalos[2]

NIST Crypto Reading Club Presentation (virtual) - October 2023

[1] Grotto Networking – (gregb@grotto-networking.com)

[2] MATTR – (vasilis.kalos@mattr.global)

BBS+ Signature Applications and Standardization

Outline Part 1

1. Introductions
2. Verifiable Credentials
3. Selective Disclosure
4. Anonymity and Unlinkability

Who Am I

My website: Grotto Networking

- Dr. Greg M. Bernstein (BS, MS, PhD UC Berkeley) - part time consultant, teacher, implementor: grotto-bbs-signatures
- Spent the pandemic teaching cybersecurity and web programming to grads and undergrads.
- Lot's of networking standards work at IETF, OIF, ITU-T, etc… Co-author/Editor of 11 IETF RFCs
- One crypto related publication and patent in early 90s
- Formerly R&D manager at big telecoms and startup

Some Key SDOs

SDOs = Standards Development Organizations

- Decentralized Identity Foundation (DIF)
- Crypto Forum Research Group (CFRG) of the IETF, note other IETF WG are interested in BBS
- World Wide Web Consortium (W3C) and their Verifiable Credential work

The BBS Name

The name **BBS** is derived from the authors of the original academic work of Dan Boneh, Xavier Boyen, and Hovav Shacham, where the scheme was first *implicitly* described in 2004.

We are *not* concerned with the original group signature here but the multi-message, unlinkable scheme more formally known as BBS+

BBS Papers and IETF Draft

- Paper 2016/663 Anonymous Attestation Using the Strong Diffie Hellman Assumption Revisited, Jan Camenisch, Manu Drijvers, and Anja Lehmann. Sections 4.3-4.5 are basis for current IETF draft.
- Paper 2023/275 Revisiting BBS Signatures, Stefano Tessaro and Chenzhi Zhu, also EUROCRYPT 2023. Optimizations and additional security proofs.
- The BBS Signature Scheme (DIF/IETF draft)

Supplemental ZKP Papers for BBS

- Schnorr Non-interactive Zero-Knowledge Proof (RFC8235), 2017. (Tutorial) Provides full details of the simplest NIZKP.
- J Camenisch and M Stadler, *Efficient group signature schemes for large groups*, 1997. *Notes*: See section 3.3 for “signature of knowledge of discrete logs”.
- J Camenisch, A Kiayias, and M Yung, *On the portability of generalized Schnorr proofs*, 2009. *Notes*: Used by CDL2016 to give the details on “poofs of knowledge of the signature”.

Extra: Quick History

1. BBS2004 *Short group signatures*, Boneh, Boyen, and Shacham
2. CL2004 *Signature Schemes and Anonymous Credentials from Bilinear Maps*, Camenisch and Lysyanskaya
3. ASM2006 *Constant-size dynamic k-TAA*, Au, Susilo, Mu
4. CDL2016 *Anonymous attestation using the strong Diffie-Hellman assumption revisited*, Camenisch, Drijvers, and Lehmann
5. TZ2023 *Revisiting BBS Signatures*, Tessaro and Zhu

BBS Demo

In browser app (no server processing) JavaScript only BBS Demo

- Uses Hex representation for all fields except messages with are UTF-8 text
- Uses JSON to hold information at various stages. These are not VCs or VPs.
- Simple list of *BBS messages* for selective disclosure, content is arbitrary

BBS Fundamental Properties 1

From DIF/IETF draft

- **SUF-CMA**: Strong unforgeability under chosen message attacks.
- **Selective Disclosure**: The scheme allows a signer to sign multiple messages and produce a single -constant size- output signature.

BBS Fundamental Properties 2

From DIF/IETF draft

- **Unlinkable Proofs**: The proofs generated by the scheme are known as zero-knowledge, proofs-of-knowledge of the signature
- **Proof of Possession**: The proofs generated by the scheme prove to a verifier that the party who generated the proof (holder/prover) was in possession of a signature without revealing it.

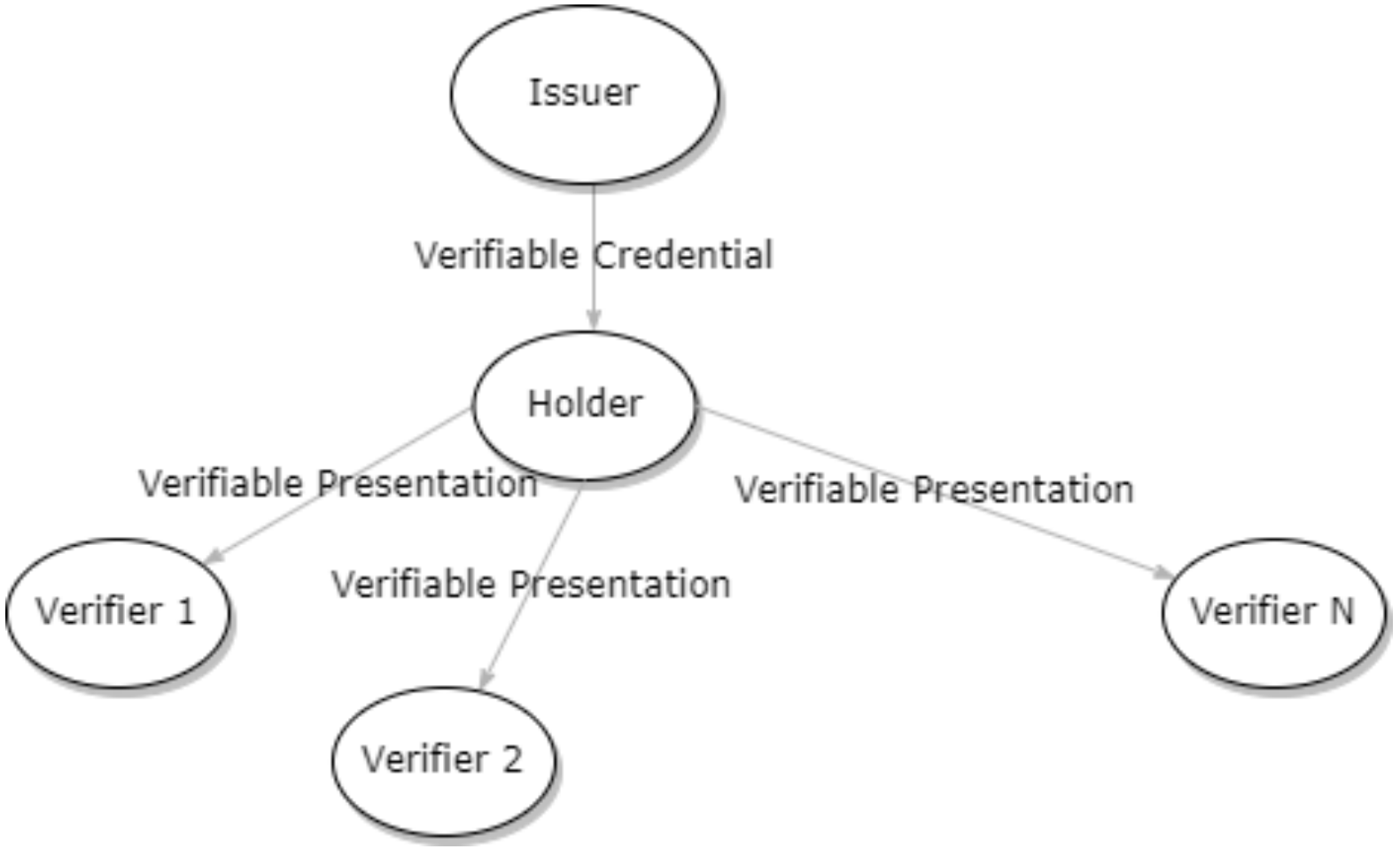
Verifiable Credentials (An Application)

Verifiable Credentials

From Verifiable Credentials Data Model v2.0 W3C Editor's Draft

Credentials are a part of our daily lives; driver's licenses are used to assert that we are capable of operating a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries. This specification provides a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable

Issuer-Holder-Verifier Model



Model with Signing (Credential and Presentation)

- **Issuer**: Signs Verifiable Credential (VC) as part of issuing process
- **Holder**: Verifies signed VC
- **Holder**: Uses a VC to create a Verifiable Presentation (VP) and sends to verifier
- **Verifier**: Verifies VP received from holder

Verifiable Credential Signature Related Specifications

- Verifiable Credential Data Integrity 1.0 Securing the Integrity of Verifiable Credential Data
- Data Integrity ECDSA Cryptosuites v1.0 Achieving Data Integrity using ECDSA with NIST-compliant curves
- Data Integrity EdDSA Cryptosuites v1.0 Achieving Data Integrity using EdDSA with Edwards curves
- BBS Cryptosuite v2023 Securing Verifiable Credentials with Selective Disclosure using BBS Signatures
- Securing Verifiable Credentials using JOSE and COSE W3C Working Draft

Example Unsigned Verifiable Credential


```
{
    "@context": [
        "https://www.w3.org/ns/credentials/v2",
        "https://www.w3.org/ns/credentials/examples/v2"
    ],
    "id": "urn:uuid:58172aac-d8ba-11ed-83dd-0b3aef56cc33",
    "type": ["VerifiableCredential", "AlumniCredential"],
    "name": "Alumni Credential",
    "description": "A minimum viable example of an Alumni
Credential.",
    "issuer": "https://vc.example/issuers/5678",
    "validFrom": "2023-01-01T00:00:00Z",
    "credentialSubject": {
        "id": "did:example:abcdefgh",
        "alumniOf": "The School of Examples"
    }
}
```

Example Signed Verifiable Credential


```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "urn:uuid:58172aac-d8ba-11ed-83dd-0b3aef56cc33",
  "type": [
    "VerifiableCredential",
    "AlumniCredential"
  ],
  "name": "Alumni Credential",
  "description": "An minimum viable example of an Alumni Credential.",
  "issuer": "https://vc.example/issuers/5678",
  "validFrom": "2023-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:example:abcdefgh",
    "alumniOf": "The School of Examples"
  },
  "proof": {
    "type": "DataIntegrityProof",
    "cryptosuite": "eddsa-2022",
    "created": "2023-02-24T23:36:38Z",
    "verificationMethod":
"https://vc.example/issuers/5678#z6MkrJVnaZkeFzdQyMZu1cgjg7k1pZZ6pvBQ7XJPt4swbTQ2",
    "proofPurpose": "assertionMethod",
    "proofValue":
"zytcLynZ8bVqCNnfw9zrGQonkmMgwRVsNiQs5WFUnUxpQsUzjT1tG27Tz9A7x8M4rGgA3nzqdQi3xjvAVhet1vFP"
  }
}
```

Hyperledger AnonCreds

- AnonCreds project page/overview
- AnonCreds Specification v1.0 Draft Uses CL signatures.
- Draft document Anonymous credentials 2.0 version 0.2, Uses BBS.
- A critique of state of AnonCreds: Being “Real” about Hyperledger Indy & Aries/Anoncreds

Selective Disclosure

Selective Disclosure and VC/VP Model

- **Issuer**: Signs VC as part of issuing process
- **Holder**: Verifies signed VC
- **Holder**: Selects what to disclose from VC (which messages in BBS terminology), constructs VP based on these choices
- **Verifier**: Verifies VP with selectively disclose information.

Selective Disclosure Approaches

Let *M* be number of messages, *U* number of undisclosed messages

- Lots of individually signed *messages*: Cost: A signature per message, i.e., *M* x *(Signature Size)
- Merkel (hash) Trees: Single signature for tree or sometimes a simple list. Presentation cost general overhead plus, worst case, a hash for each undisclosed message *U* x *(Hash size)*
- BBS: Fixed signature size, Presentation cost: general overhead and a scalar (32 bytes) per undisclosed message, i.e., *U* x *(32 bytes)*

Higher Level Selective Disclosure Protocols

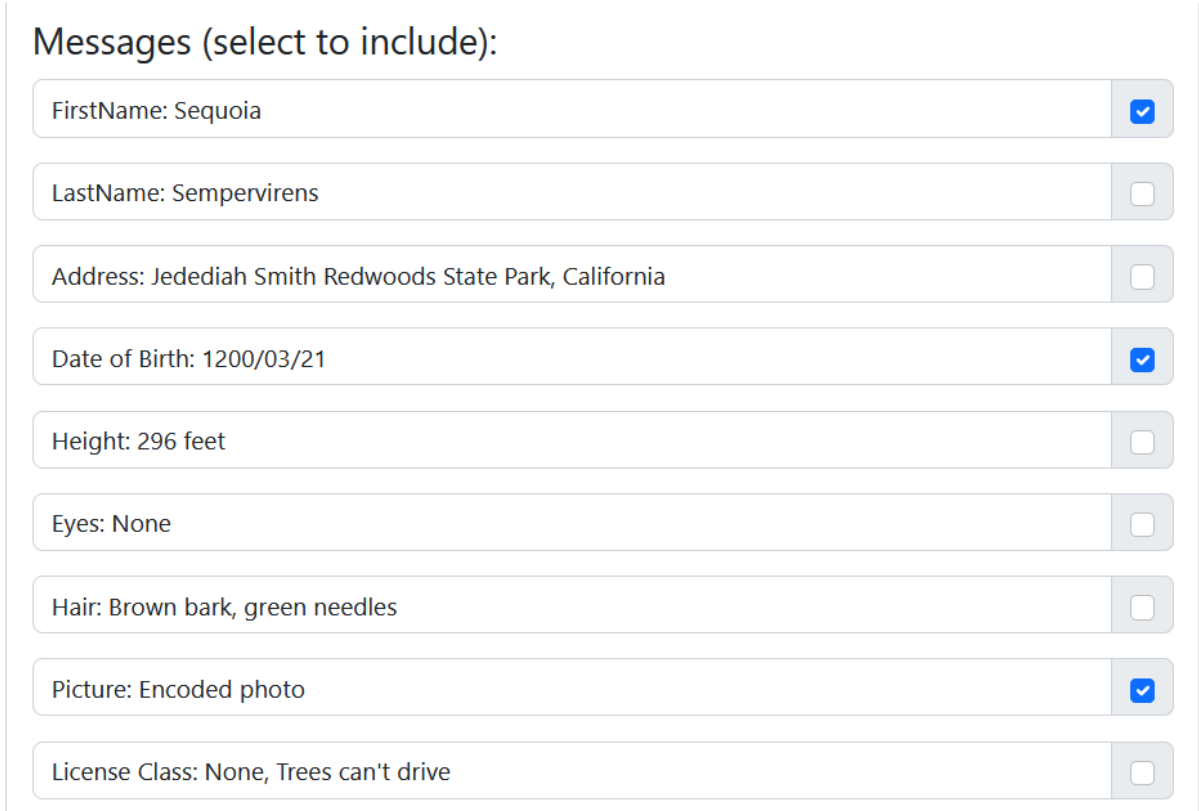
- Selective Disclosure for JWTs (SD-JWT) IETF Draft.
- JSON Web Proof IETF Draft, (supports BBS as well as other cryptographic approaches).
- ECDSA-SD and SD-primitives in Data Integrity ECDSA Cryptosuites v1.0 Achieving Data Integrity using ECDSA with NIST-compliant curves.

BBS Example: Tree Drivers License

From [Grotto BBS demo](), not a VC or mDL…


```
{
  "publicKey":
"b65b7cbff4e81b723456a13936b6bcc77a078bf6291765f3ae13170072249dd7daa7ec1bd82b818ab601980
30b45b8fa159c155fc3841a9ad4045e37161c9f0d9a4f361b93cfdc67d365f3be1a398e56aa173d7a55e01b4
a8dd2494e7fb90da7",
  "header": "11223344556677889900aabbccddeeff",
  "messages": [
    "FirstName: Sequoia",
    "LastName: Sempervirens",
    "Address: Jedediah Smith Redwoods State Park, California",
    "Date of Birth: 1200/03/21",
    "Height: 296 feet",
    "Eyes: None",
    "Hair: Brown bark, green needles",
    "Picture: Encoded photo",
    "License Class: None, Trees can't drive"
  ],
  "signature":
"94bb93062e05bc702d0ab222b861fd0311533d6dcbcad4050e45dd2392de951a912915af08bd87b22848074
32245f9960e1f59680a59cd9fae490dee659d63fd3922a728e2ba3ee33db6bcc806ec2cea3d7264489a42ca0
9deeac7ca88b1811c2158b51d81560832daf6a0000037a87a"
}
```

BBS Example: A Tree goes to a bar…



Selective Disclosure

BBS Example Derived “Proof”

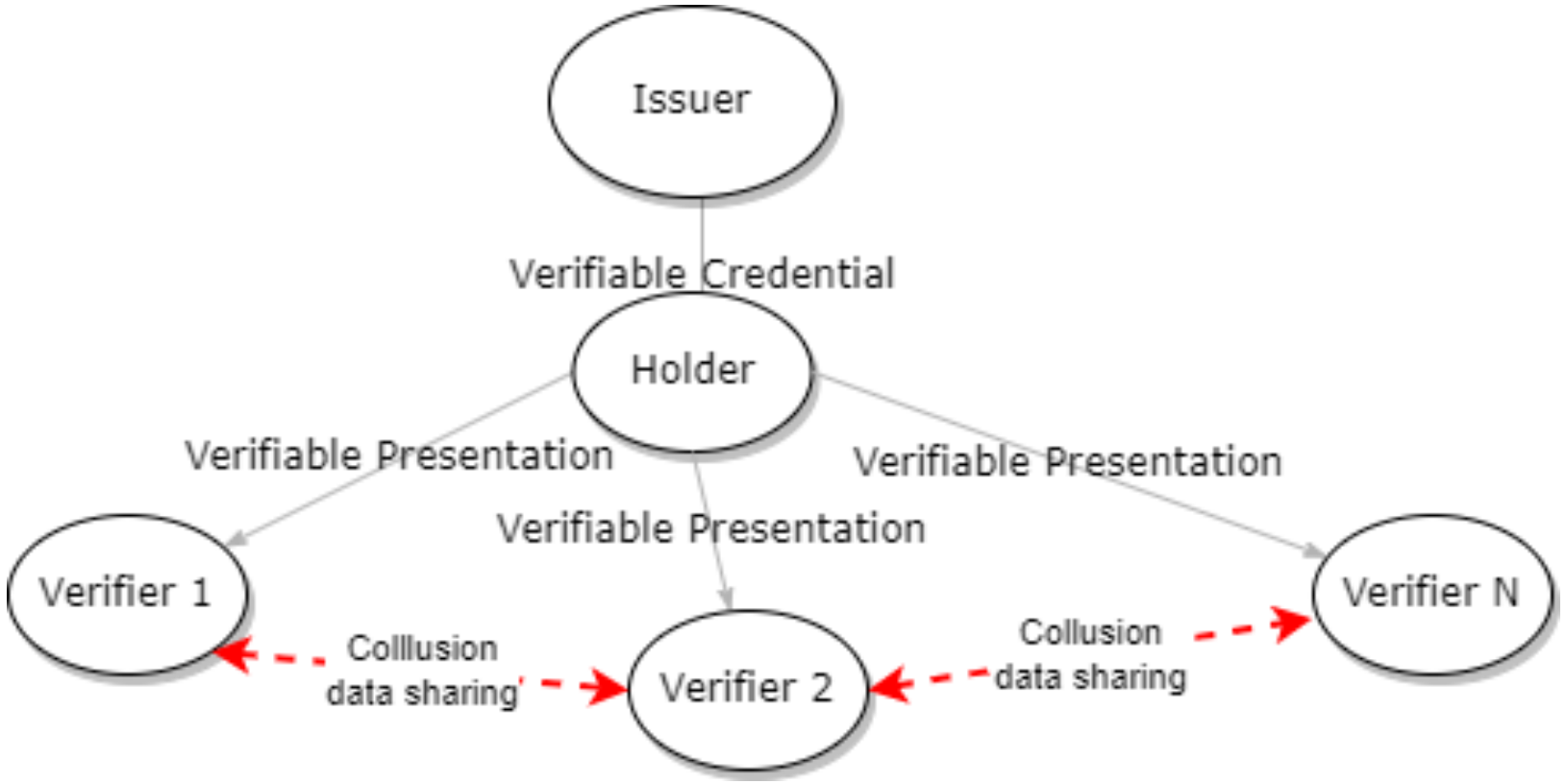

```
{
  "pk":
"b65b7cbff4e81b723456a13936b6bcc77a078bf6291765f3ae13170072249dd7daa7ec1bd82b818ab60198030b45b8fa159c1
55fc3841a9ad4045e37161c9f0d9a4f361b93cfdc67d365f3be1a398e56aa173d7a55e01b4a8dd2494e7fb90da7",
  "header": "112233445566778899 00aabbccddeeff",
  "ph": "",
  "disclosedIndexes": [
    0,
    3,
    7
  ],
  "disclosedMsgs": [
    "FirstName: Sequoia",
    "Date of Birth: 1200/03/21",
    "Picture: Encoded photo"
  ],
  "proof":
"a6089a46f59e005a11885fe29e8e67679d6545b42e1126858ef2a3b6cbd5b2f1de1577194ce57077bfb1d555476e10a8afb64
592f6e37e2e9f2f99422c7b6466cc49499f2e0a7d670a19a0e3765e6522b95376c06a776965a81e29238c3c9350b0e367daa23
010490da97c2002027b43c6f7ba181f601eb4462964883c08e4ffcb9424180aaadc103f89c923d88b88c4015ff3d28a64887a8
8ae0944d3aaf1ed371173f068b3d0b79a5177c287b1c64271807cc03d331a3b18d3491898a1be13c6404cae9acbacd7ce635a4
d7a6b520b1a33fb1ca1dbcbc90158269b2e2a58714fc97c892a5ebd839fb22f307d29bdf822b21bf1a906b428ee75f0dc408eb
bb4085e6f4e057bb3b1f783e636e0de07eb542e2d1054e89b0451148bf703a9e59cce2e49e000d8aa1448acd514393d7f661b0
28cdbaec607bef03384028f6a47907c0d1e2b16c03e37c73b75b2d6d85a670186be482b4abbc2cecc90d29b16c11a12eeededc
68fc16e0729e97a14d44a5e6cedca243afad6024d46f7fa738e635ff3e93c5502ad3b7772c1f0bc86d5fa930a34ea0771bddb3
a9da5e308613b468421de3dc6789ae5c014915199d978082615a81214f0efb12fc824b3a1b5c9ab2ba7b62a4e44ef21eabe9fb
f2803d13d360730c49c8e5c67617b739593e0824fc0f2e626f30e88d365007df318571b467b"
}
```

Anonymity and Unlinkability

Holders and Verifiers

- An issuer signs a VC by including a cryptographic signature. By their security properties these tend to be “unique”
- When a holder creates a VP that includes the signed VC the cryptographic signature is included.
- If a holder sends this VP to multiple verifiers and those verifiers share data, i.e., collude, then the holder’s activities can be **tracked** or **worse**. **Verifier-Verifier** collusion.
- Or a verifier could send this information back to the issuer. **Verifier-Issuer** collusion.

Verifiers-Verifier Tracking

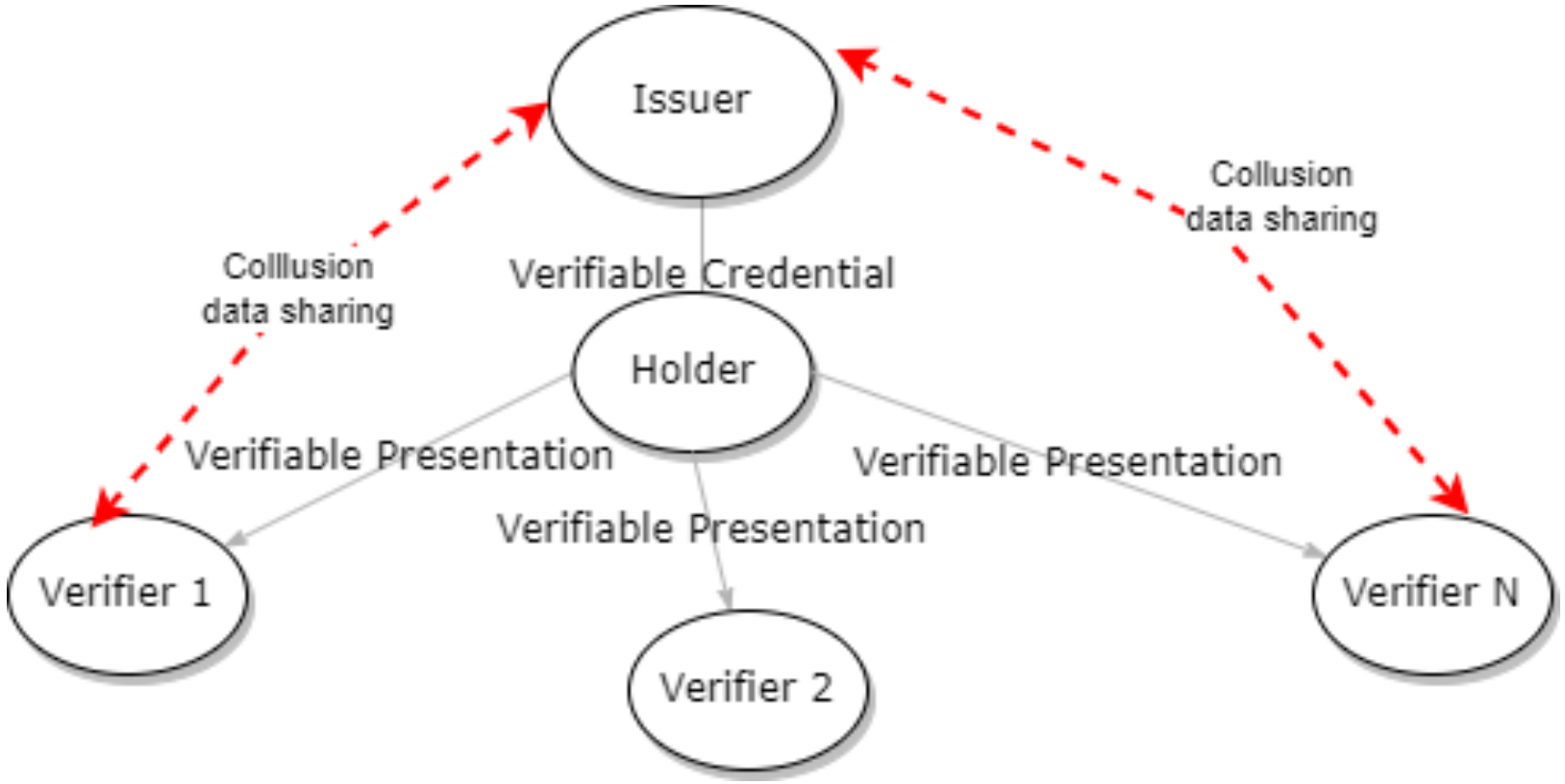


Verifier Collusion

Does this really happen?

- Cover your Tracks Try out their tool to see how unique your computer/browser combination is
- Mozilla: What is fingerprinting
- NPM: FingerprintJS 300K downloads a week…

Verifier-Issuer Tracking



Verifier-Issuer Collusion

Federated Identity Management Systems

From Wikipedia: Verifiable Credentials

The federated identity management (FIM) model, as adopted by SAML and OpenID Connect, places the identity provider (IdP) in the central role as the dispenser of identity attributes and the determiner of which Service Providers (SPs) it will give them to. In the federated model, the IdP knows every SP that the user visits.

Proposed and Existing National Identity Systems

- Modular Open Source Identity Platform (MOSIP) Has mechanisms to prevent **Verifier-Verifier** collusion but not, currently, **Verifier-Issuer** collusion.
- MOSIP is being deployed in India, Bhutan, etc… See MOSIP News for recent announcements of more countries.
- Toward Mending Two Nation-Scale Brokered Identification Systems LTAN Brandão, N Christin, G Danezis, Proceedings on Privacy Enhancing Technologies 2015 (2), 135-155

Unlinkable Proofs Example 1

- A tree goes into a bar and needs to prove it lives in a local state park in order to get a very large glass of water.
- It then goes to another local bar for another very large glass of water.
- It doesn’t want to be tracked across bars or have its water consuming habits tracked.
- Solution: Generate a separate **BBS proof** for each bar it visits

Unlinkable Proofs Example 2

BBS Proof presented at first bar


```
{
  "pk":
"b65b7cbff4e81b723456a13936b6bcc77a078bf6291765f3ae13170072249dd7daa7ec1bd82b818ab60198030b45b8fa159c1
55fc3841a9ad4045e37161c9f0d9a4f361b93cfdc67d365f3be1a398e56aa173d7a55e01b4a8dd2494e7fb90da7",
  "header": "112233445566778899aabbccddeeff",
  "ph": "",
  "disclosedIndexes": [
    2
  ],
  "disclosedMsgs": [
    "Address: Jedediah Smith Redwoods State Park, California"
  ],
  "proof":
"a312e2476de36c0fc2a815ebd9236c6cc1831a3fcdb3d2cdaf4d3ff325259a4d36e910ea06b75f6708f035924c6488da989a5
7fbbcfe187e78d2550f23eabb577a3c2457147cbf68f82f16c75ba9b52ea0e36d264a7ac3304fb8892ad9c4c33ea2505ffb8c9
aaa203094bf2bd917c1c18c62fd3b7c7459616dced8836d3d5f608201c7d0b7a80daf8205d2451bd33d5b06fab9f3dda846137
539b4ae53d9dbaf699bb3f43f9ab38d936e8f4d035128af0e19867e3edcfeb58175d44ac6a4f471b2bca58d9b4de80291b2809
658a804f570e9d7e0aa55bf157d138cdd6a82b7364db5443e1fa5fc9d52f404097d85889755761f48befdcb5d2d581d2911808
e9d6b4b213b7eeb4c38b878195f13b004ba1179b5a7f88cc39aeca21ab781a5107c4e69b29db00876274df71d4460f09dfd3df
287bb384c6efb9c6fd3cbb7f0f0d3545b07c5a039686ac1a10b7eb0cf52f46e28d38f970dccf6f4d039b78a11f42349a52d063
97a10ed80ac567ee29f21e6022200ca71c088cf7bada1878150cd776716f66495ff0337e72572a325329539466cc3d17450347
98b0a09e1c62090f3be3d4a22b518aff620a484d0bd5461f95c5ca7e5a8f50ddb96e29dda0192def462c611bccb9465c3457e1
b69bce4b6676e190be338e030da06b481014271828eee6648b40626f4b293980e4267b22c39121236376dc2e786f92ba760d21
f174068028e87c29e7167a5023295a4af6a8141ba8c5de8dd25e2f1b8b7fdfa72d60324c6c81e2ca3951dc761b75e10d05646"
}
```

Unlinkable Proofs Example 3

BBS Proof presented at second bar


```
{
  "pk":
"b65b7cbff4e81b723456a13936b6bcc77a078bf6291765f3ae13170072249dd7daa7ec1bd82b818ab60198030b45b8fa159c1
55fc3841a9ad4045e37161c9f0d9a4f361b93cfdc67d365f3be1a398e56aa173d7a55e01b4a8dd2494e7fb90da7",
  "header": "112233445566778899aabbccddeeff",
  "ph": "",
  "disclosedIndexes": [
    2
  ],
  "disclosedMsgs": [
    "Address: Jedediah Smith Redwoods State Park, California"
  ],
  "proof":
"8175e24b57337bd8abed395c0d2440efe71e55cf06fbb1ead5d4e8589e2a5dc295688f561851d5f2e169a417c2ddde32b7801
550cb442227db1503f1dfdf803125c9f10aae16b69ec58ad33a0ff9acc18405f0f24640e5381a2abadefcc6fb6e952bbd8ec90
8a60c28dc5913a25a586ee9b49f9a8fec0eff51dafc283ea44d07dd60292e6ef5711a202ef055fa7a203f727bdf0087f1b91d9
6a91e07ca417eed8cc03f00a1de1b013ceff998d9a6ff55559105abc53a80b30d68eb644150602f55cfb3de0bc949d9d3c8573
2df6d5d1535798679d0d29895bfe1ef58d9aa63f0fc160394a5739c65602d9bb21fffa4ed27408be6c0beb579b997eb0426d85
fc3c7db1961992e85df1fd35cd421dc007b130d9f41568b7d9984689c883ea9a8b6e50b95c8cfd1bee71f2ad1c08cb2134b533
7794d6a387aefc44af1929e456d857197d02acf1caddbd751380a9ac5a00c10c6df911dd00bc27e4d68dc6af5023e83e2e45f8
0b416b98d7d46ea967835c3155f3b6a22fcb8534a23b15c16805ae4adb98bfd17bc096a9ad0636dbdb844344c862d44b5d8d55
d4fa0be73623ce5f1ea558cdb1e8dc8f4b958a8bda851115802a3b12ce54177b236dd98d819a2dbeafa1a04e0214fbb3bccb5e
df94e0c9cfa575334bf48ffa11755435bc40945fc46e862f67c8f5ee6247f9f9a3c57dbd4122551605f3db005764db0717e2f8
365a8458141c94549db43c8034798532817582507b679e7fc724518e281443a0f1d59c9d030df6e8ef65cd33093919ae1a018"
}
```

Unlinkable Proofs Limitations

- The values (cryptographic byte array) contained in the *BBS proofs* are unlinkable. In particular they appear essentially random
- Unlinkable proofs do not prevent correlation on disclosed messages or **artifacts** from higher layers of a protocol stack!

BBS Signatures - Theory

What Can BBS do??

A lot...

- Selective Disclosure ✓
- Unlinkability ✓
- Threshold Signatures ✓
- Holder Binding ✓
- Blind Signatures ✓
- Pseudonyms ✓
- Predicate Proofs ✓
- Anonymous revocation ✓
- Group Signatures ✓
- DAA ✓

What Can BBS do??

A lot...

- Selective Disclosure ✓
- Unlinkability ✓
- Threshold Signatures ✓
- Holder Binding ✓
- Blind Signatures ✓
- Pseudonyms ✓
- Predicate Proofs ✓
- Anonymous revocation ✓
- Group Signatures ✓
- DAA ✓

What Can BBS do??

A lot...

- Selective Disclosure ✓
- Unlinkability ✓
- Threshold Signatures ✓
- Holder Binding ✓
- Blind Signatures ✓
- Pseudonyms ✓
- Predicate Proofs ✓
- Anonymous revocation ✓
- Group Signatures ✓
- DAA ✓

What Can BBS do??

A lot...

- Selective Disclosure ✓
- Unlinkability ✓
- Threshold Signatures ✓
- Holder Binding ✓
- Blind Signatures ✓
- Pseudonyms ✓
- Predicate Proofs ✓
- Anonymous revocation ✓
- Group Signatures ✓
- DAA ✓

What Can BBS do??

A lot...

- Selective Disclosure ✓
- Unlinkability ✓
- Threshold Signatures ✓
- Holder Binding ✓
- Blind Signatures ✓
- Pseudonyms ✓
- Predicate Proofs ✓
- Anonymous revocation ✓
- Group Signatures ✓
- DAA ✓

What Can BBS do??

A lot...

- Selective Disclosure ✓
- Unlinkability ✓
- Threshold Signatures ✓
- Holder Binding ✓
- Blind Signatures ✓
- Pseudonyms ✓
- Predicate Proofs ✓
- Anonymous revocation ✓
- Group Signatures ✓
- DAA ✓

…and more!

BBS Signatures – The Math

Issue, Verify, Present and Verify Presentation

BBS Signatures: Preliminaries

Groups:

- Prime p
- Groups G_1, G_2, G_T with order p.
- Let $rep(.)$ be the representation size of a group's point, then:

$$rep(G_1) < rep(G_2) < rep(G_T)$$

Pairings:

- Bilinear function e: $G_1 \times G_2 \rightarrow G_T$
- $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$
- Pairing type:
  - Type 1: $G_1 = G_2$
  - Type 2: $G_1 \neq G_2$ but homomorphic
  - Type 3: $G_1 \neq G_2$ and not homomorphic

Efficiency

BBS Signatures: Preliminaries

- Prime p
- Groups $G_1 \neq G_2 \neq G_T$ of order p
- Pairing $e: G_1 \times G_2 \rightarrow G_T$
- Generators $g_1 \in G_1$ and $g_2 \in G_2$

q-SDH

Given $[g_1, g_1^x, g_1^{x^2}, \ldots, g_1^{x^q}, g_2, g_2^x]$ Calculate $g_1^{\frac{1}{x+e}}$ for some $e \in Z_p$

In G_1 In G_2

How to sign messages $M = (m_1, m_2, \ldots, m_L)$??

Make g_1 a commitment to M

BBS Signatures: Issuance

- Prime p
- Groups $G_1 \neq G_2 \neq G_T$ of order p
- Pairing $e: G_1 \times G_2 \rightarrow G_T$
- Generators $g_1 \in G_1$ and $g_2 \in G_2$

q-SDH $\left\{ \text{Given } \left[g_1, g_1^x, g_1^{x^2}, \ldots, g_1^{x^q}, g_2, g_2^x\right] \xrightarrow{\text{Calculate}} g_1^{\frac{1}{x+e}} \text{ for some } e \in Z_p \right\}$

- Secret key $x \xleftarrow{\$} Z_p^*$, Public key $PK = g_2^x$
- Sign messages $M = (m_1, m_2, \ldots, m_L)$
  1. Sample generators $h_1, h_2, \ldots, h_L \xleftarrow{\$} G_1$ — Deterministically created from constant seed and a PRF
  2. Sample $e \xleftarrow{\$} Z_p$ — Deterministically created from x and M
  3. Calculate A as,

$$A = \left(g_1 h_1^{m_1} h_2^{m_2} \cdots h_L^{m_L} \right)^{\frac{1}{x+e}}$$

Signature on $M \rightarrow (A, e)$

BBS Signatures: Verification

- Prime p
- Groups $G_1 \neq G_2 \neq G_T$ of order p
- Pairing $e: G_1 \times G_2 \rightarrow G_T$
- Generators $g_1 \in G_1$ and $g_2 \in G_2$

q-SDH $\left\{ \text{Given } \left[g_1, g_1^x, g_1^{x^2}, \ldots, g_1^{x^q}, g_2, g_2^x\right] \xrightarrow{\text{Calculate}} g_1^{\frac{1}{x+e}} \text{ for some } e \in Z_p \right\}$

- Secret key $x \xleftarrow{\$} Z_p^*$, Public key $PK = g_2^x$
- Sign messages $M = (m_1, m_2, \ldots, m_L)$

$$A = \left(g_1 h_1^{m_1} h_2^{m_2} \cdots h_L^{m_L} B \right)^{\frac{1}{x+e}}$$

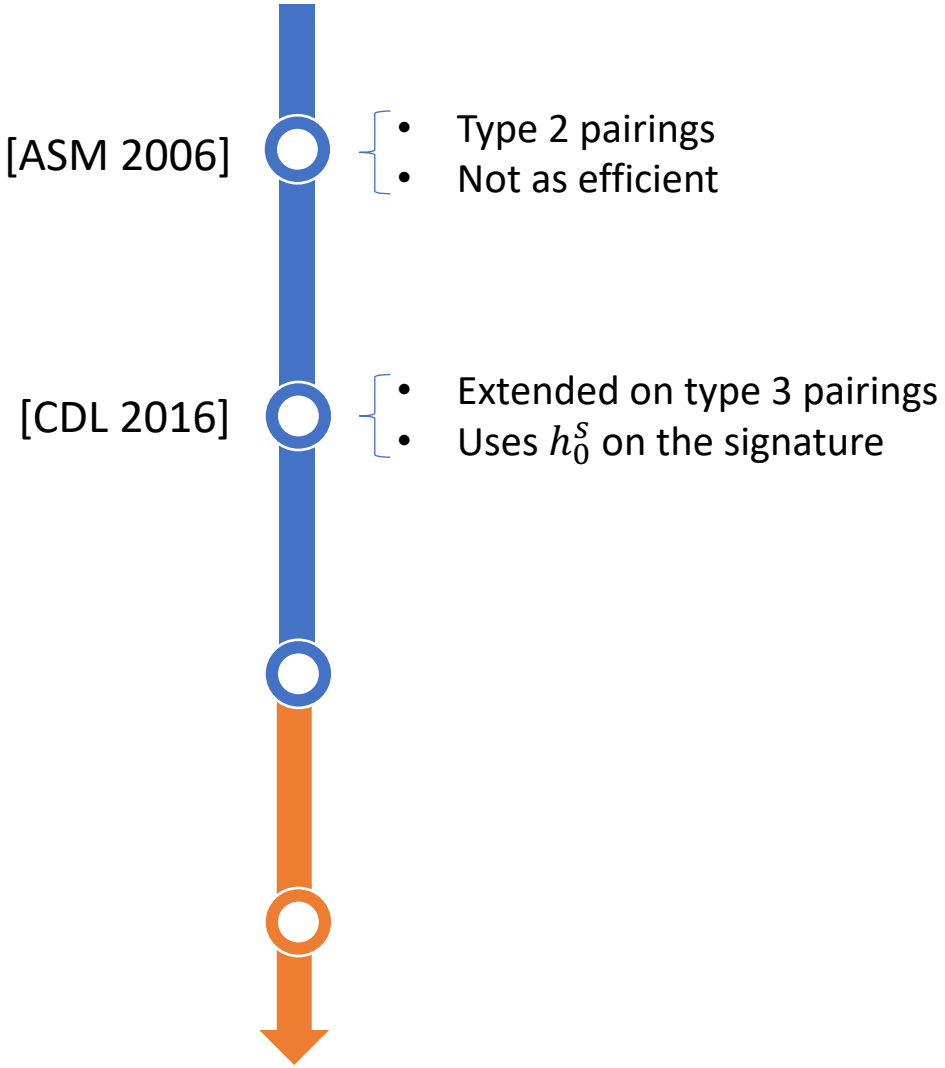
Verify

$$e(A, g_2^e PK) = e(B, g_2)$$

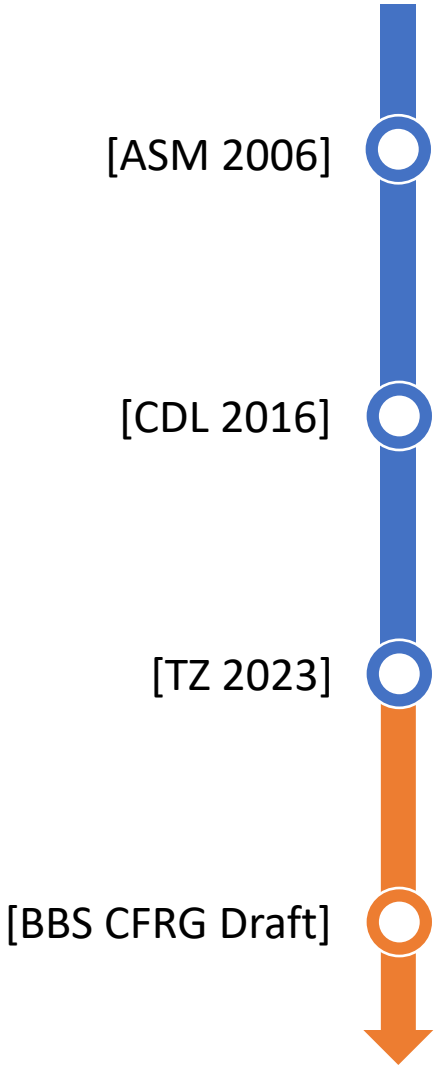
$$e\left(B^{\frac{1}{x+e}}, g_2^{e+x}\right) = e(B, g_2)$$

BBS PoK & Selective Disclosure

The Chronicles of the BBS PoK



The Chronicles of the BBS PoK



[ASM 2006]

- Type 2 pairings
- Not as efficient

[CDL 2016]

- Extended on type 3 pairings
- Uses h_0^s on the signature

[TZ 2023]

- SUF without h_0^s
- PoK security reduced to q-SDH

[BBS CFRG Draft]

- Uses alternative PoK
- Security not reduced to q-SDH
- Easy to combine with other ZKPs

Remnant of the [CDH16] PoK for weak Boneh-Boyen signatures ([BB07]).

$$A = \left(g_1 h_0^s h_1^{m_1} \cdots h_L^{m_L}\right)^{\frac{1}{e+x}} \rightarrow (A, e, s)$$

BBS Signatures: Proof Generation

- Public key $PK = g_2^x$
- Signature (A, e) on $M = (m_1, m_2, \ldots, m_L)$

$$B = g_1 h_1^{m_1} h_2^{m_2} \cdots h_L^{m_L}$$

$$A = \left(B \right)^{\frac{1}{x+e}}$$

BBS Signatures: Proof Generation

- Public key $PK = g_2^x$
- Signature (A, e) on $M = (m_1, m_2, \dots, m_L)$

$$B = g_1 h_1^{m_1} h_2^{m_2} \cdots h_L^{m_L} \qquad r_1, r_2 \xleftarrow{\$} Z_p$$

$$A = \left(B \right)^{\frac{1}{x+e}}$$

Blind A ⟹ $\overline{A} = A^{r_1 r_2}$

Blind B ⟹ $D = B^{r_2}$

$$\overline{A}^{x+e} = B^{r_1 r_2} \Rightarrow \overline{A}^{x} = D^{r_1} \overline{A}^{-e}$$

Set $\overline{B} = D^{r_1} \overline{A}^{-e} \rightarrow \overline{B} = \overline{A}^{x}$

Prove this with an SPK

Prove this with pairings

BBS Signatures: Proof Generation

- Public key $PK = g_2^x$
- Signature (A, e) on $M = (m_1, m_2, \dots, m_L)$

$$A = \left(g_1 h_1^{m_1} h_2^{m_2} \cdots h_L^{m_L} \right)^{\frac{1}{x+e}} = B^{\frac{1}{x+e}}$$

Present

$Dis \subseteq [L]$

PoK Gen Steps

- $D = B^{r_2}$
- $\overline{A} = A^{r_1 r_2}$
- $\overline{B} = D^{r_1} \overline{A}^{-e}$ $(= \overline{A}^{x})$
- Calculate π as:

$\pi = SPK\{(e, r_1),$

$\overline{B} = D^{r_1} \overline{A}^{-e}\}$

$\overline{A}^{x+e} = B^{r_1 r_2} \Rightarrow$

$\Rightarrow \overline{A}^{x} = D^{r_1} \overline{A}^{-e}$

BBS Signatures: Proof Generation

- Public key $PK = g_2^x$
- Signature (A, e) on $M = (m_1, m_2, \dots, m_L)$

$$A = \left(g_1 h_1^{m_1} h_2^{m_2} \cdots h_L^{m_L} \right)^{\frac{1}{x+e}} = B^{\frac{1}{x+e}}$$

Present

$Dis \subseteq [L]$

PoK Gen Steps

- $D = B^{r_2}$
- $\overline{A} = A^{r_1 r_2}$
- $\overline{B} = D^{r_1} \overline{A}^{-e}$ $(= \overline{A}^{x})$
- Calculate π as:

$\overline{A}^{x+e} = B^{r_1 r_2} \Rightarrow$
$\Rightarrow \overline{A}^{x} = D^{r_1} \overline{A}^{-e}$

$$\pi = SPK\{(e, r_1, r_2^{-1}, \{m_i\}_{i \notin Dis}),$$

$$\overline{B} = D^{r_1} \overline{A}^{-e}$$

$$\wedge$$

$$g_1 \prod_{i \in Dis} h_i^{m_i} = D^{r_2^{-1}} \prod_{i \notin Dis} h_i^{-m_i}\}$$

Proof of correctness of D

$$\Rightarrow proof = (\overline{A}, \overline{B}, D, \pi)$$

BBS Signatures: Proof Verification

- Public key $PK = g_2^x$

Proves that $\overline{B} = \overline{A}^x$

PoK Verify Steps

- Check that $e(\overline{A}, PK) = e(\overline{B}, g_2)$
- Validate π

=> $proof = (\overline{A}, \overline{B}, D, \pi)$

Validate

$Dis \subseteq [L]$

Proves knowledge of $e, r_1, r_2^{-1}, \{m_i\}_{\{i \notin Dis\}}$ so that

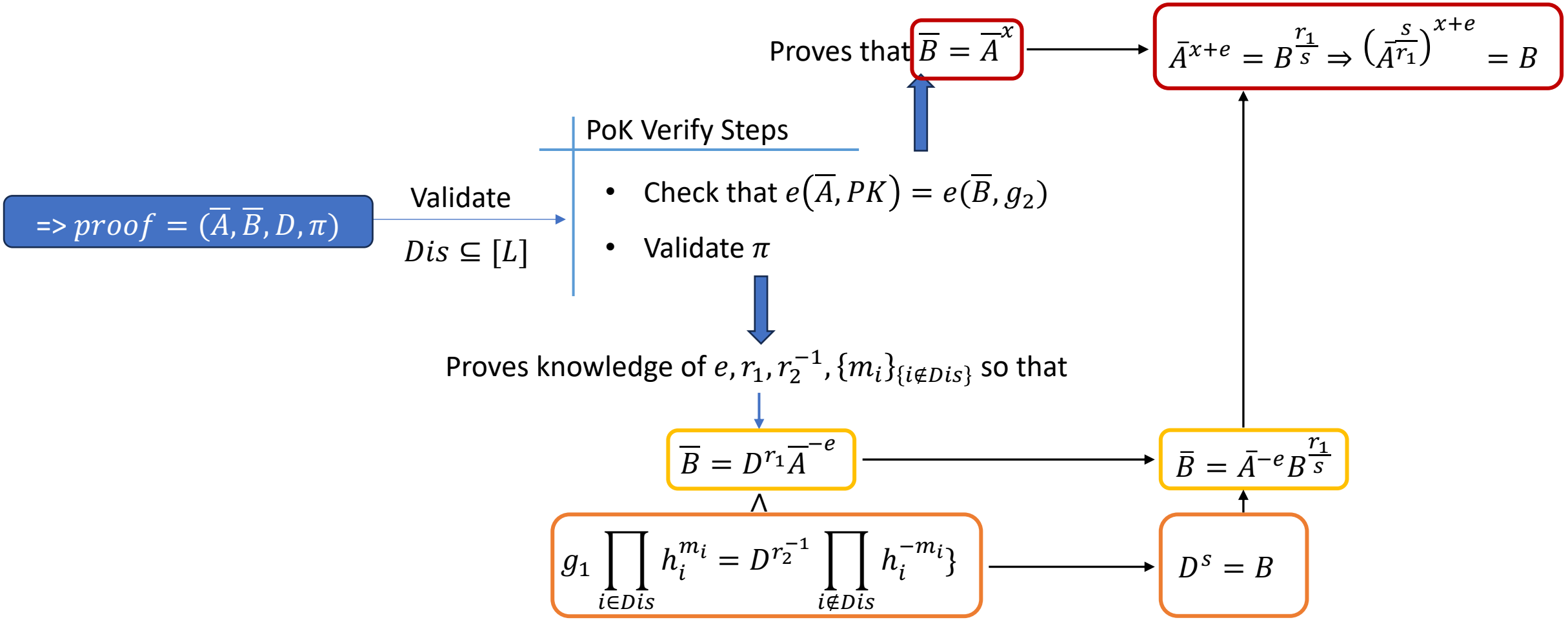
$$\overline{B} = D^{r_1}\overline{A}^{-e}$$

$$\wedge$$

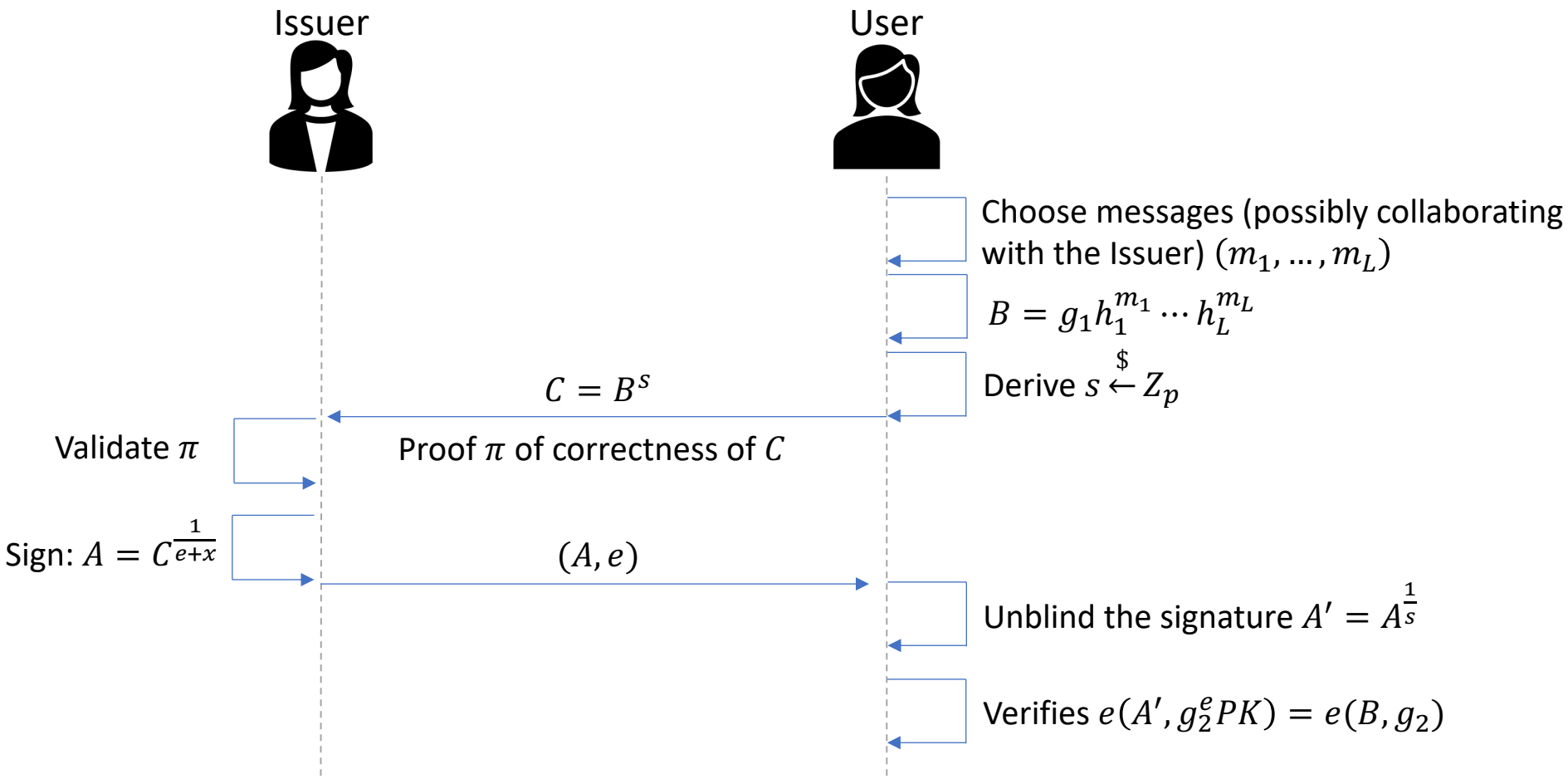
$$g_1 \prod_{i \in Dis} h_i^{m_i} = D^{r_2^{-1}} \prod_{i \notin Dis} h_i^{-m_i}\}$$

BBS Signatures: Proof Verification

- Public key $PK = g_2^x$



Blind BBS Signatures



Blind BBS Signatures

Issuer

User

Choose messages (possibly collaborating with the Issuer) $(m_1, \dots, m_L)$

$B = g_1 h_1^{m_1} \cdots h_L^{m_L}$

Derive $s \xleftarrow{\$} Z_p$

$C = B^s$

Validate π

Proof π of correctness of C

Sign: $A = C^{\frac{1}{e+x}}$

(A, e)

Unblind the signature $A' = A^{\frac{1}{s}}$

Verifies $e(A', g_2^e PK) = e(B, g_2)$

- The Issuer will not know the signature A'
- Will come into play in PQ security…

BBS Signatures with Fewer Pairings [BBDT17]

During Signature Verification

Checking that $A^{x+e} = B\ (= g_1 h_1^{m_1} h_2^{m_2} \cdots h_L^{m_L})$ with:

$$e(A, g_2^e PK) = e(B, g_2)$$

Replaced with

- Issuer publishes: $PK' = h^X$
- Issuer calculates: $\hat{\pi} = SPK\{(x), BA^{-e} = A^x \ \wedge \ PK' = h^x\}$
- Adds $\hat{\pi}$ to the signature: $(A, e, \hat{\pi})$

Verify proof by validating $\hat{\pi}$ with PK'

During Proof Verification

Checking that $\bar{A}^x = \bar{B}$ with:

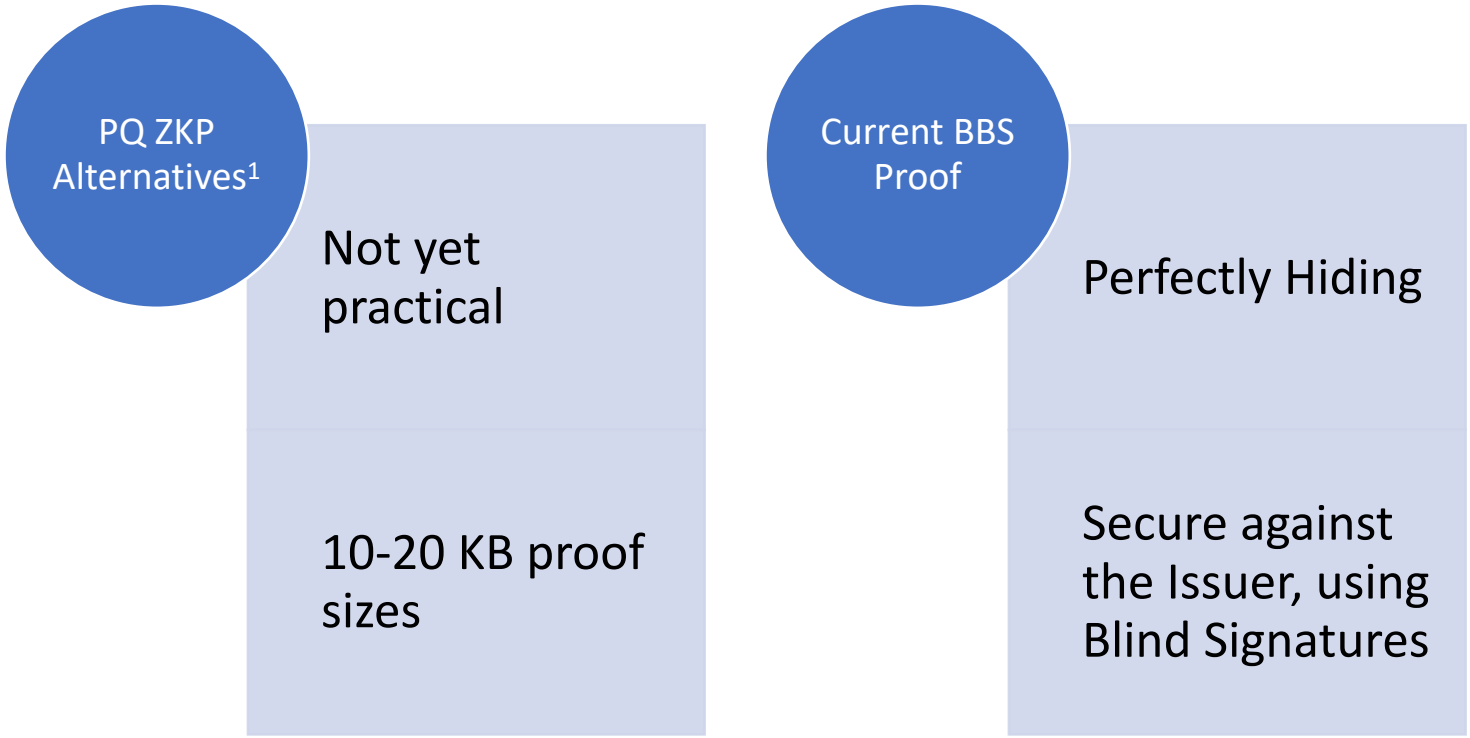
$$e(\bar{A}, PK) = e(\bar{B}, g_2)$$

Replaced with

- If Issuer := Verifier (i.e., the Verifier knows x)

Directly check that $\bar{A}^x = \bar{B}$

BBS in the Post Quantum Word



1. e.g., [KZ22]

Anonymous Credential Protocols

	Space Efficiency (bytes)				Time Efficiency		
	Secret key	Public Key	Signature	Presentation	Sign	Present	Verify presentation
CL[1] (2056 RSA)	257	$640 + N * 128$	661	$661 + U * 256$	$N - ME.QR_n$	$N - ME.QR_n$	$N - ME.QR_n$
PS[2] (BLS12381)	$(N + 1) * 32$	$(N + 1) * 96$	96	$128 + U * 32$	$1 - ME.G_1$	$N - ME.G_T + N{\times}P$	$N - ME\ G_T + N{\times}P$
SD-JWT[3] (ES256)	32	32	64	$64 + N * 32$	$1 - ME.G_1$	–	$2 - ME.G_1$
BBS (BLS12381)	**32**	**48**	**80**	$\boldsymbol{272 + U * 32}$	$\boldsymbol{N - ME.G_1}$	$\boldsymbol{N - ME.G_1}$	$\boldsymbol{N - ME.G_1 + 2{\times}P}$

- $\boldsymbol{n - ME.G}$: Size n multi-exponentiation in the group G.
- $\boldsymbol{N}$: Number of signed messages.
- $\boldsymbol{U}$: Number of un-disclosed messages.

1. [CL03]
2. [PS16]
3. [SD-JWT Draft]

Anonymous Credential Protocols

	Space Efficiency (bytes)				Time Efficiency		
	Secret key	Public Key	Signature	Presentation	Sign	Present	Verify presentation
CL[1] (2056 RSA)	257	$640 + N * 128$	661	$661 + U * 256$	$N - ME.QR_n$	$N - ME.QR_n$	$N - ME.QR_n$
PS[2] (BLS12381)	$(N + 1) * 32$	$(N + 1) * 96$	96	$128 + U * 32$	$1 - ME.G_1$	$N - ME.G_T + N{\times}P$	$N - ME\ G_T + N{\times}P$
SD-JWT[3] (ES256)	32	32	64	$64 + N * 32$	$1 - ME.G_1$	$-$	$2 - ME.G_1$
BBS (BLS12381)	**32**	**48**	**80**	$\boldsymbol{272 + U * 32}$	$\boldsymbol{N - ME.G_1}$	$\boldsymbol{N - ME.G_1}$	$\boldsymbol{N - ME.G_1 + 2{\times}P}$

- $\boldsymbol{n - ME.G}$: Size n multi-exponentiation in the group G.
- $\boldsymbol{N}$: Number of signed messages.
- $\boldsymbol{U}$: Number of un-disclosed messages.

1. [CL03]
2. [PS16]
3. [SD-JWT Draft]

Anonymous Credential Protocols

	Space Efficiency (bytes)				Time Efficiency		
	Secret key	Public Key	Signature	Presentation	Sign	Present	Verify presentation
CL[1] (2056 RSA)	257	$640 + N * 128$	661	$661 + U * 256$	$N - ME.QR_n$	$N - ME.QR_n$	$N - ME.QR_n$
PS[2] (BLS12381)	$(N + 1) * 32$	$(N + 1) * 96$	96	$128 + U * 32$	$1 - ME.G_1$	$N - ME.G_T + N \times P$	$N - ME\ G_T + N \times P$
SD-JWT[3] (ES256)	32	32	64	$64 + N * 32$	$1 - ME.G_1$	–	$2 - ME.G_1$
BBS (BLS12381)	**32**	**48**	**80**	$\boldsymbol{272 + U * 32}$	$\boldsymbol{N - ME.G_1}$	$\boldsymbol{N - ME.G_1}$	$\boldsymbol{N - ME.G_1 + 2 \times P}$

SD-JWT Verifier-Verifier Unlinkability: Possible through tokenization

- Works great for low-velocity use cases (e.g., mDL) 👍
- Problematic for high-velocity use cases (e.g., web-based applications, privacy pass, privacy-preserving access tokens etc.) 👎
  - Increased infrastructure requirments.
  - Rate limiting, Token Hording attacks, Token Exostion attacks etc.

SD-JWT Verifier-Issuer Unlinkability: Not supported 👎

➢ BBS are better suited

1. [CL03]
2. [PS16]
3. [SD-JWT Draft]

References

[CL03] Camenisch, J., & Lysyanskaya, A. (2003). A signature scheme with efficient protocols. In *Security in Communication Networks: Third International Conference, SCN 2002 Amalfi, Italy, September 11–13, 2002 Revised Papers 3* (pp. 268-289). Springer Berlin Heidelberg.

[ASM06] Au, M. H., Susilo, W., & Mu, Y. (2006). Constant-Size Dynamic k-TAA. In *Security and Cryptography for Networks: 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006. Proceedings 5* (pp. 111-125). Springer Berlin Heidelberg.

[BB08] Boneh, D., & Boyen, X. (2008). Short Signatures Without Random Oracles and the SDH Assumption in Bilinear Groups. *Journal of cryptology*, *21*(2), 149-177.

[CDL16] Camenisch, J., Drijvers, M., & Lehmann, A. (2016). Anonymous Attestation Using the Strong Diffie Hellman Assumption Revisited. In *Trust and Trustworthy Computing: 9th International Conference, TRUST 2016, Vienna, Austria, August 29-30, 2016, Proceedings 9* (pp. 1-20). Springer International Publishing.

[CDH16] Camenisch, J., Drijvers, M., & Hajny, J. (2016). Scalable Revocation Scheme for Anonymous Credentials Based on n-times Unlinkable Proofs. In *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society* (pp. 123-133).

[PS16] Pointcheval, D., & Sanders, O. (2016). Short randomizable signatures. In *Topics in Cryptology-CT-RSA 2016: The Cryptographers' Track at the RSA Conference 2016, San Francisco, CA, USA, February 29-March 4, 2016, Proceedings* (pp. 111-126). Springer International Publishing.

[BBDT17] Barki, A., Brunet, S., Desmoulins, N., & Traoré, J. (2017). Improved Algebraic MACs and Practical Keyed-Verification Anonymous Credentials. In *Selected Areas in Cryptography–SAC 2016: 23rd International Conference, St. John's, NL, Canada, August 10-12, 2016, Revised Selected Papers 23* (pp. 360-380). Springer International Publishing.

[KZ22] Kales, D., & Zaverucha, G. (2022). Efficient lifting for shorter zero-knowledge proofs and post-quantum signatures. *Cryptology ePrint Archive*.

[TZ23] Tessaro, S., & Zhu, C. (2023). Revisiting BBS Signatures. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 691-721). Cham: Springer Nature Switzerland.

[SD-JWT Draft] Fett, D., Yasuda, K., & Campbell, B. (2022). Selective Disclosure for JWTs (SD-JWT). Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/

[BBS CFRG Draft] Looker, T., Kalos, V., Whitehead, A., & Lodder, M. (2022). The BBS Signature Scheme. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/>

References

[BBS04] Boneh, D., Boyen, X., & Shacham, H. (2004). Short Group Signatures. In *Annual International Cryptology Conference* (pp. 41-55). Berlin, Heidelberg: Springer Berlin Heidelberg.

[CL04] Camenisch, J., & Lysyanskaya, A. (2004). Signature Schemes and Anonymous Credentials from Bilinear Maps. In *Annual International Cryptology Conference* (pp. 56-72). Berlin, Heidelberg: Springer Berlin Heidelberg.

[DKLS23] Doerner, J., Kondi, Y., Lee, E., Shelat, A., & Tyner, L. (2023, May). Threshold BBS+ Signatures for Distributed Anonymous Credential Issuance. In *2023 IEEE Symposium on Security and Privacy (SP)* (pp. 773-789). IEEE.

Thank You!