Asiacrypt 2024

Adaptor Signatures: New Security Definition and A Generic Construction for NP Relations

Xiangyu Liu, **Ioannis Tzannetos**, Vassilis Zikas

Adaptor Signature Scheme

Signature scheme:

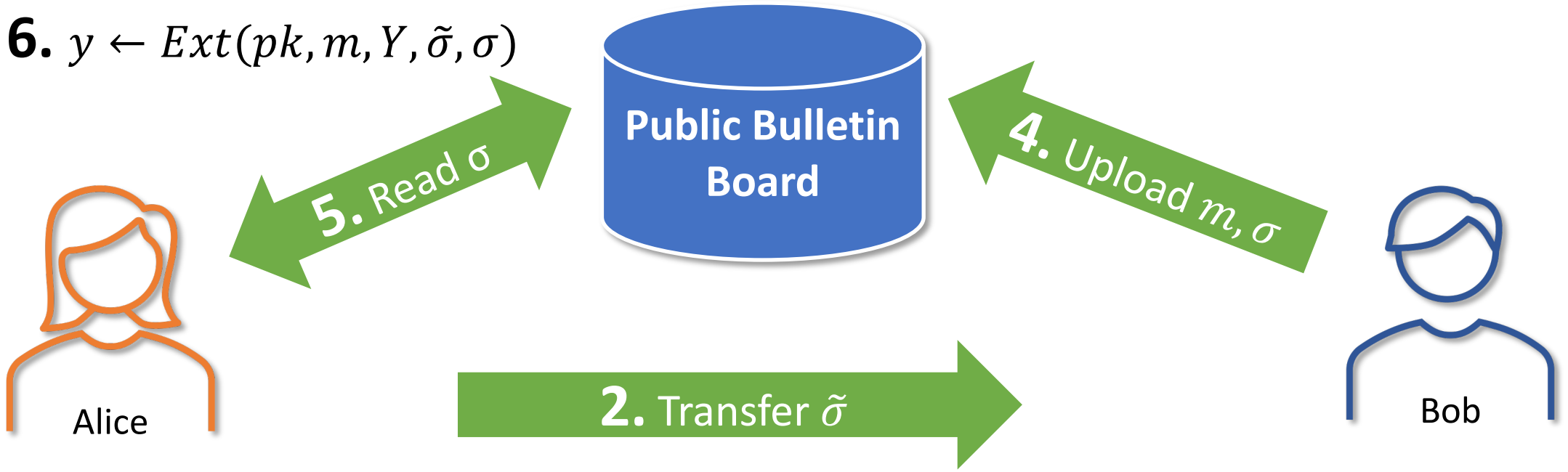
- key generation: $(pk, sk) \leftarrow Gen(1^{\lambda})$
- sign: $\sigma \leftarrow Sign(sk, m)$
- verification: $0/1 \leftarrow Ver(pk, m, \sigma)$

Adaptor Signature (AS) scheme w.r.t. hard relation R:

- pre-sign: $\tilde{\sigma} \leftarrow pSign(sk, m, Y)$
- pre-verification: $0/1 \leftarrow pVer(pk, m, Y, \tilde{\sigma})$
- adaption: $\sigma \leftarrow Adapt(pk, m, \tilde{\sigma}, y)$
- extraction: $y/\perp \leftarrow Ext(pk, m, Y, \tilde{\sigma}, \sigma)$

$(Y, y) \in R$
Y an instance (statement)
y a witness of Y

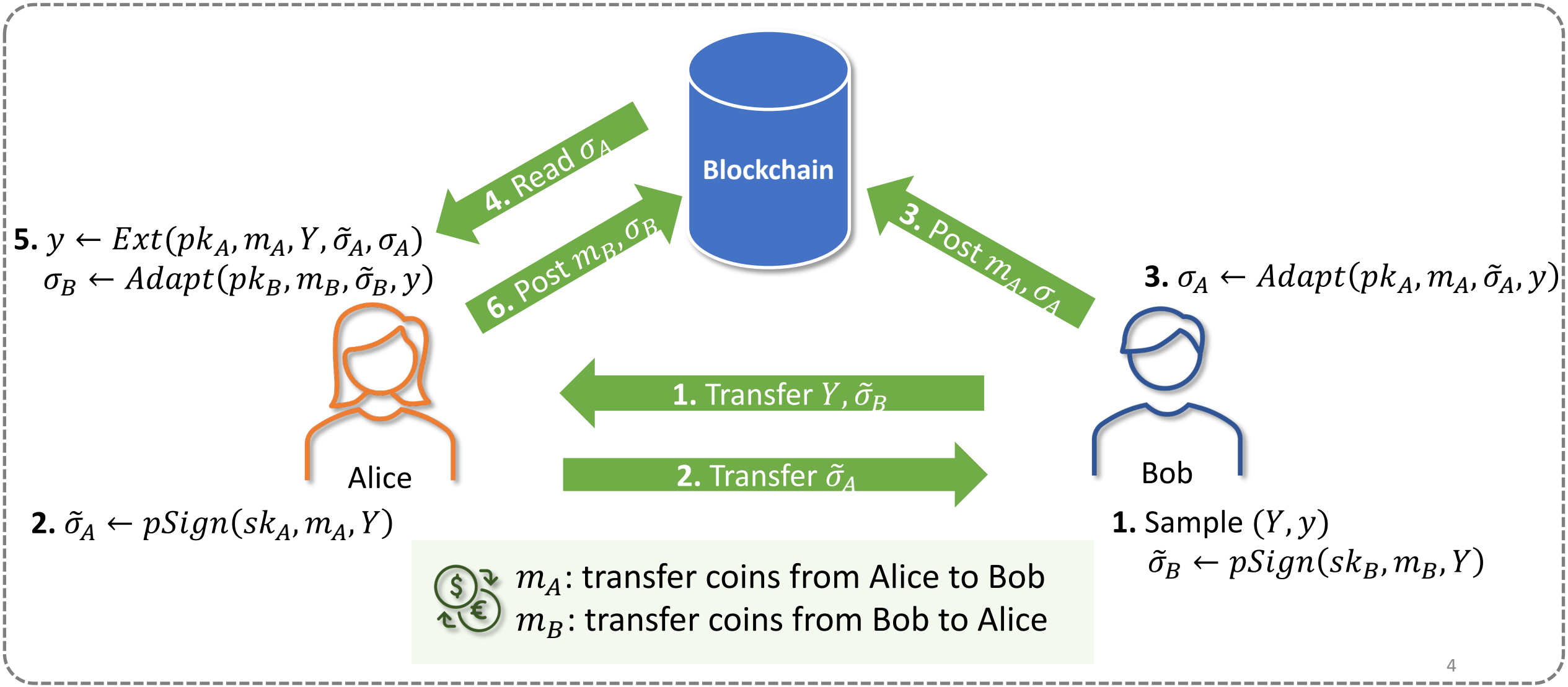
Adaptor Signatures



Alice knows (pk, sk) and statement Y
and wants the witness y

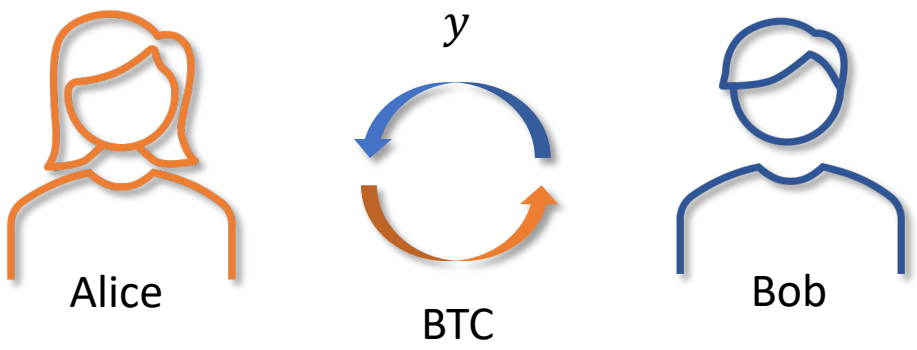
Bob knows (Y, y)
and wants a signature (of Alice) on m

Atomic Swaps based on Adaptor Signatures

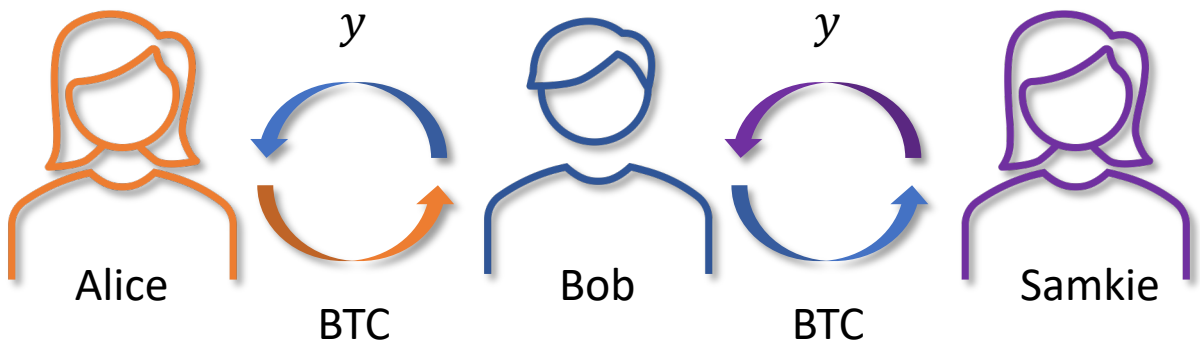


More Applications of AS

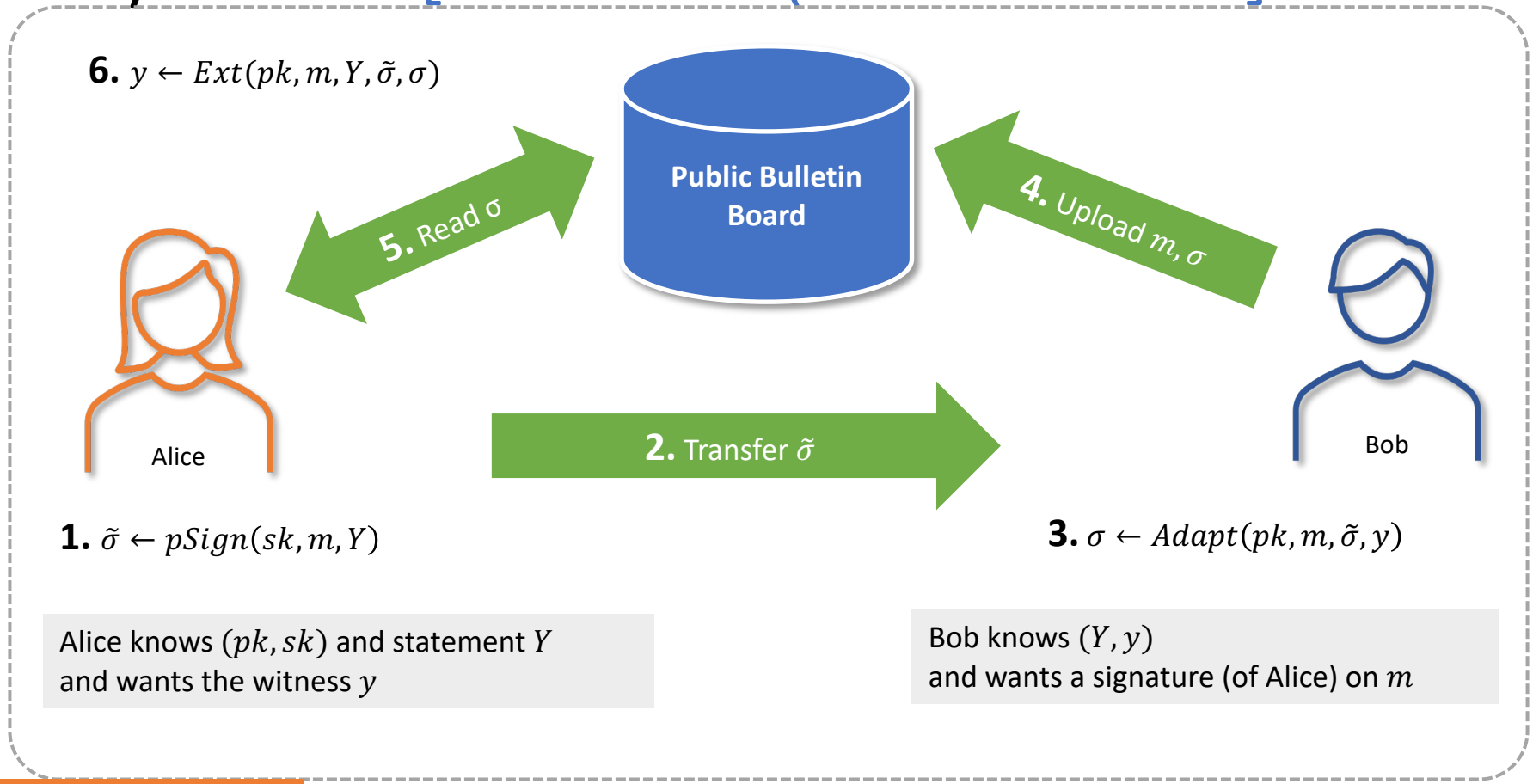
✓ Witness for a coin



✓ Multi-hop payments



Security of AS [AEE+21 (ASIACRYPT]

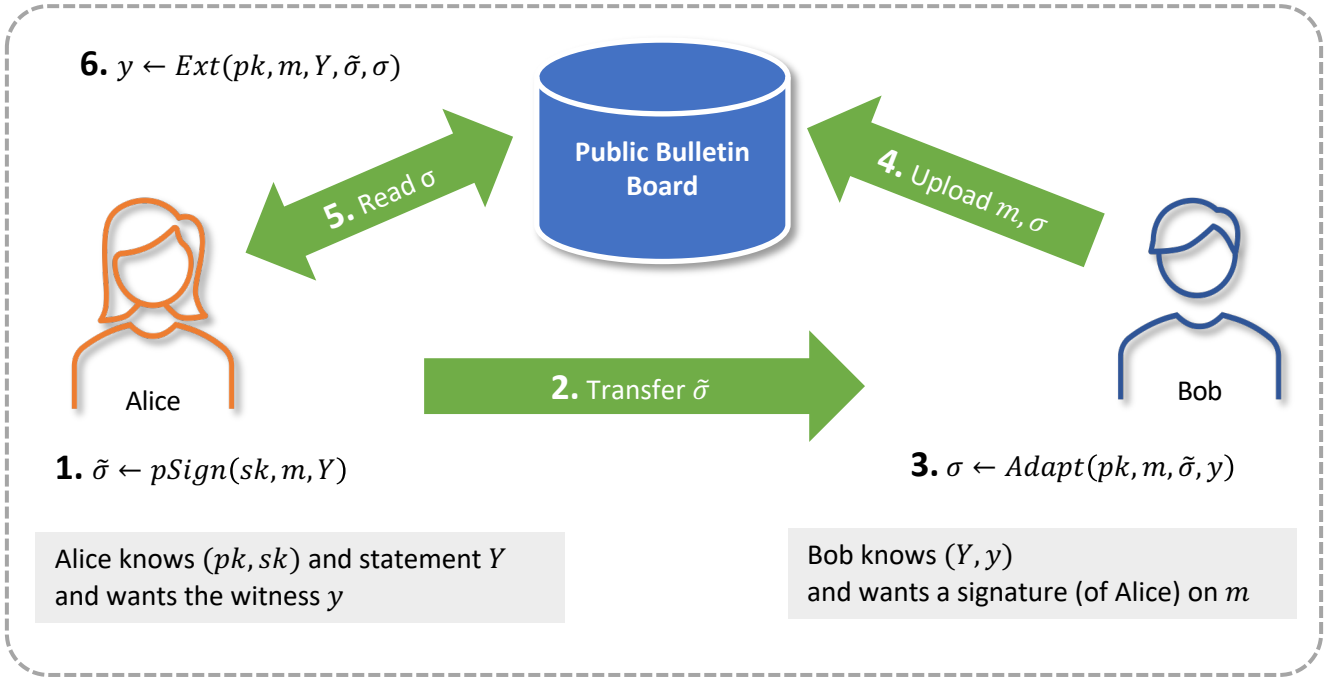


Sender's security:
witness extractability

+Unforgeability

Receiver's security
pre-signature adaptability

Security of AS



+Unforgeability

Sender's security (witness extractability): Sender can extract a witness from the valid pre-signature and adapted signature

Receiver's security (pre-signature adaptability): Receiver can adapt a valid pre-signature into a full signature with witness y

Related Works

- ECDSA-based AS [AEE+21 (ASIACRYPT]
- Schnorr-based AS [AEE+21 (ASIACRYPT), TZC22 (ISC)]
- LWE/SIS-based scheme LAS [EEE20 (ESORICS)]
- Code-based scheme AS [KH22 (Cryptogr)]
- Isogeny-based scheme IAS [TMM21 (FC)]
- Identification (ID) schemes based AS [EFH+21, (PKC)]

Related Works (AS for NP)

The next natural question is can we have adaptor signatures for all NP ?

Dai et al. [DOY22 (INDOCRYPT)] answered to the affirmative.

Let SIG be a normal signature scheme

- Pre-signature: $\tilde{\sigma} = (\bar{\sigma}, Y)$ s.t. $\bar{\sigma} \leftarrow SIG.Sign(sk, (m, Y))$
- (Full) signature: $\sigma = (\bar{\sigma}, Y, y)$

The verification algorithm checks the validity of

1. $SIG.ver(pk, (m, Y), \bar{\sigma})$
2. $(Y, y) \in R$

Dai's Construction

(Full) signature: $\sigma = (\bar{\sigma}, Y, y)$

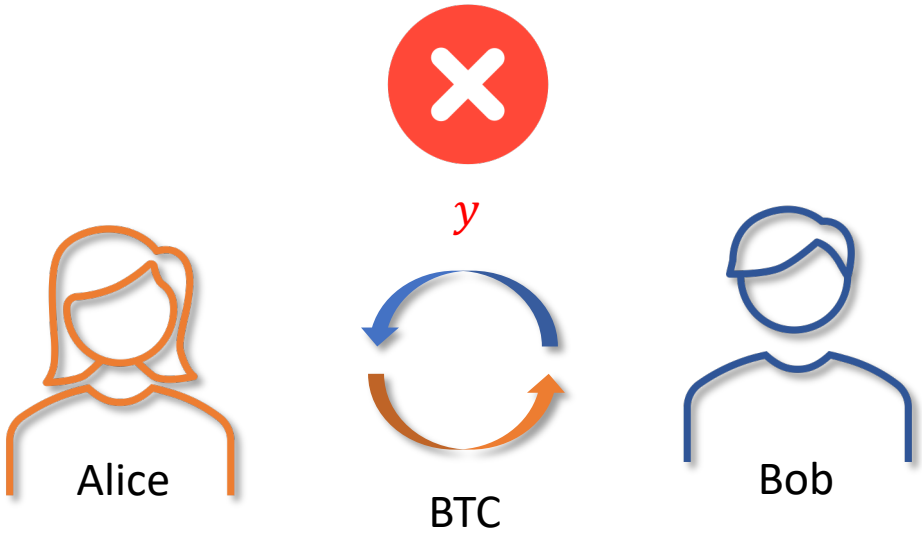
While simple it satisfies all security notions of AS:

- ❖Unforgeability
- ❖Witness Extractability
- ❖Pre-signature adaptability

Though it comes with a security risk:

- ❖The witness is **exposed** in **plain!**

Why is witness exposure a problem?



New Security Notion: Witness Hiding

- witness y can be extracted from both a pre-signature and an adapted signature (jointly), but not from only one of them alone

An adaptor signature scheme AS w.r.t. relation R is witness hiding, if there exists a simulator Sim such that, for any PPT adversary $\mathcal{A}$,

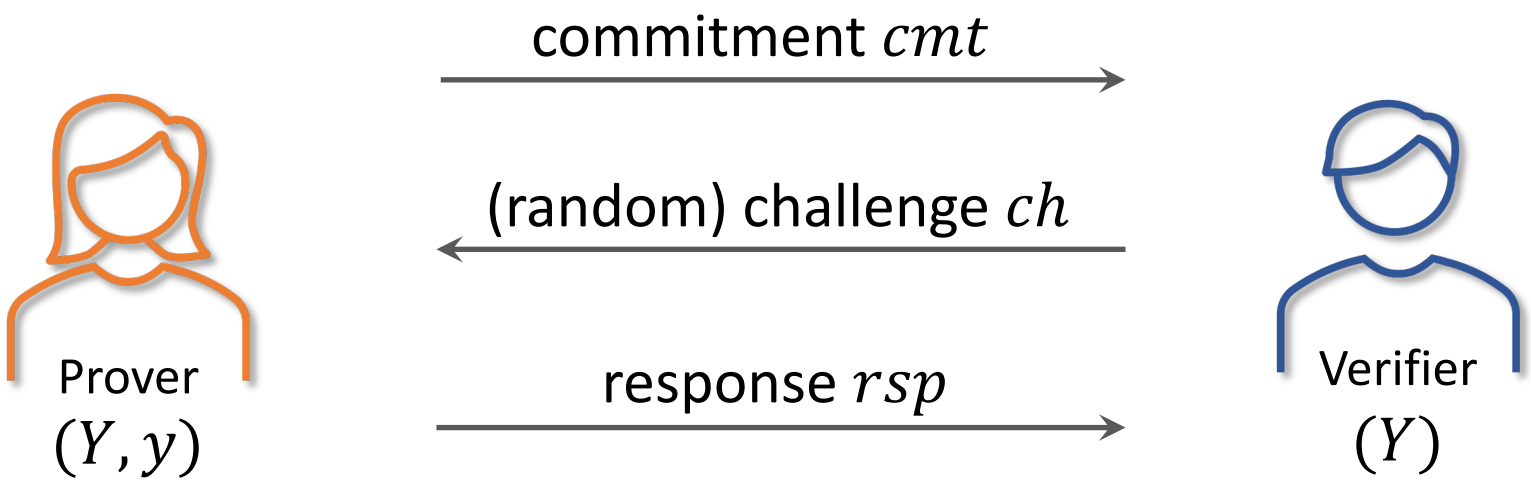
$$\mathsf{Adv}^{wh}_{\mathsf{AS},\mathsf{Sim}\mathcal{A}}(\lambda) := |\Pr[\mathsf{Exp}^{wh}_{\mathsf{AS},\mathsf{Sim},\mathcal{A},0}(\lambda) \Rightarrow 1] - \Pr[\mathsf{Exp}^{wh}_{\mathsf{AS},\mathsf{Sim},\mathcal{A},1}(\lambda) \Rightarrow 1]|$$

is negligible over λ, where $\mathsf{Exp}^{wh}_{\mathsf{AS},\mathsf{Sim},\mathcal{A},b}(\lambda)$ $(b \in \{0,1\})$ is defined below

$\underline{\mathsf{Exp}^{wh}_{\mathsf{AS},\mathsf{Sim},\mathcal{A},b}(\lambda)}$:	$\underline{\textsc{Chall}_0(pk, sk, m)}$	$\underline{\textsc{Chall}_1(pk, sk, m)}$
$(Y, y) \leftarrow \mathsf{Sample}(R)$	If $f_{\mathsf{AS}}(pk, sk) \neq 1$: Return $\perp$	If $f_{\mathsf{AS}}(pk, sk) \neq 1$: Return $\perp$
Return $\mathcal{A}^{\textsc{Chall}_b(\cdot,\cdot,\cdot)}(Y)$	// check the validity of (pk, sk)	// check the validity of (pk, sk)
	$\tilde{\sigma} \leftarrow \mathsf{pSign}(sk, m, Y)$	$\sigma \leftarrow \mathsf{Sim}(pk, sk, m, Y)$
	$\sigma \leftarrow \mathsf{Adapt}(pk, m, \tilde{\sigma}, y)$	Return σ
	Return σ	

Question : Can we have *witness-hiding* adaptor signatures for all NP ?

Witness-hiding AS vs. Sigma protocols



A transcript = (cmt, ch, rsp)

- **Special soundness of Sigma protocols**. From two valid transcripts with the same commitment but different challenges, one can extract a witness

- **Witness extractability of AS**. From a valid pre-signature and an adapted signature one can extract a witness

Designing AS for NP Relations

- Let SIG be a normal signature scheme
- Now the pre-signature

$$\tilde{\sigma} \leftarrow (\bar{\sigma}, Y, (cmt, ch, rsp)) \text{ s.t } \begin{cases} \bar{\sigma} \leftarrow SIG.sign\big(sk, (m, Y, cmt)\big) \\ (cmt, ch, rsp) \text{ is a transcript for proving } y \end{cases}$$

- With witness y, $\tilde{\sigma}$ is adapted to

$$\sigma \leftarrow (\bar{\sigma}, Y, (cmt, ch' \neq ch, rsp'))$$

- Zero-knowledge of Sigma protocol $\Longrightarrow$ witness hiding

Observation: ch in the pre-signature can be fixed!

Designing AS for NP Relations

- Define dummy message $m_{\mathbf{0}}$, and now

  $\tilde{\sigma} \leftarrow (\bar{\sigma}, Y, (cmt, ch = m_{\mathbf{0}}, rsp))$ s.t $\begin{cases} \bar{\sigma} \leftarrow SIG.sign(sk, (m, Y, cmt)) \\ (cmt, ch, rsp) \text{ is a transcript for proving } y \end{cases}$

- With witness y, $\tilde{\sigma}$ is adapted to

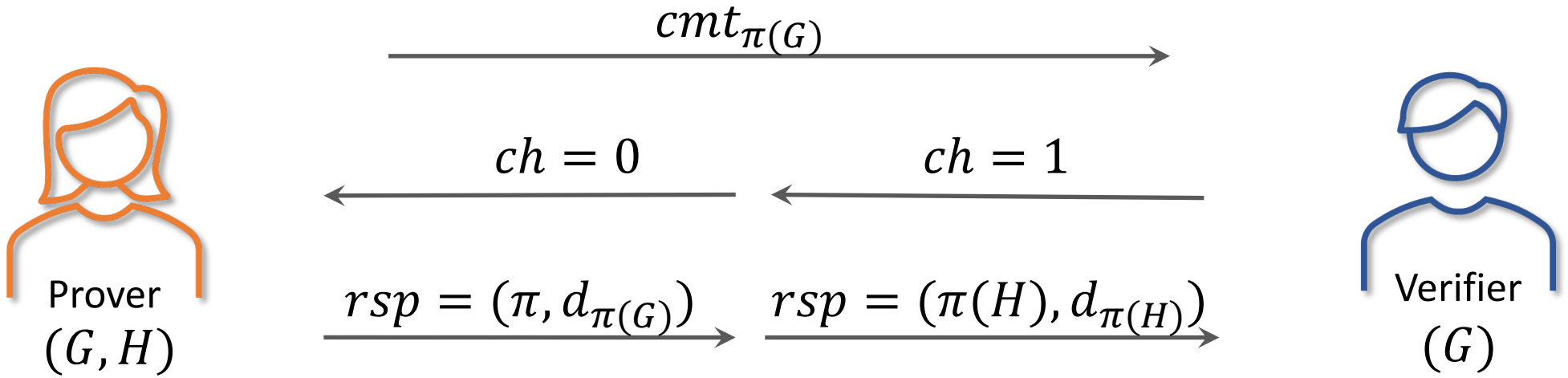
  $\sigma \leftarrow (\bar{\sigma}, Y, (cmt, m \neq m_{\mathbf{0}}, rsp'))$

We need:

✓ the commitment is not related to the witness

✓ given the commitment for dymmy $m_{\mathbf{0}}$ and witness, one can open this commitment to any other message as the challenge

Blum's Sigma Protocol for Hamiltonian Cycle



d: the opening of a commitment

- The commitment is not related to the witness

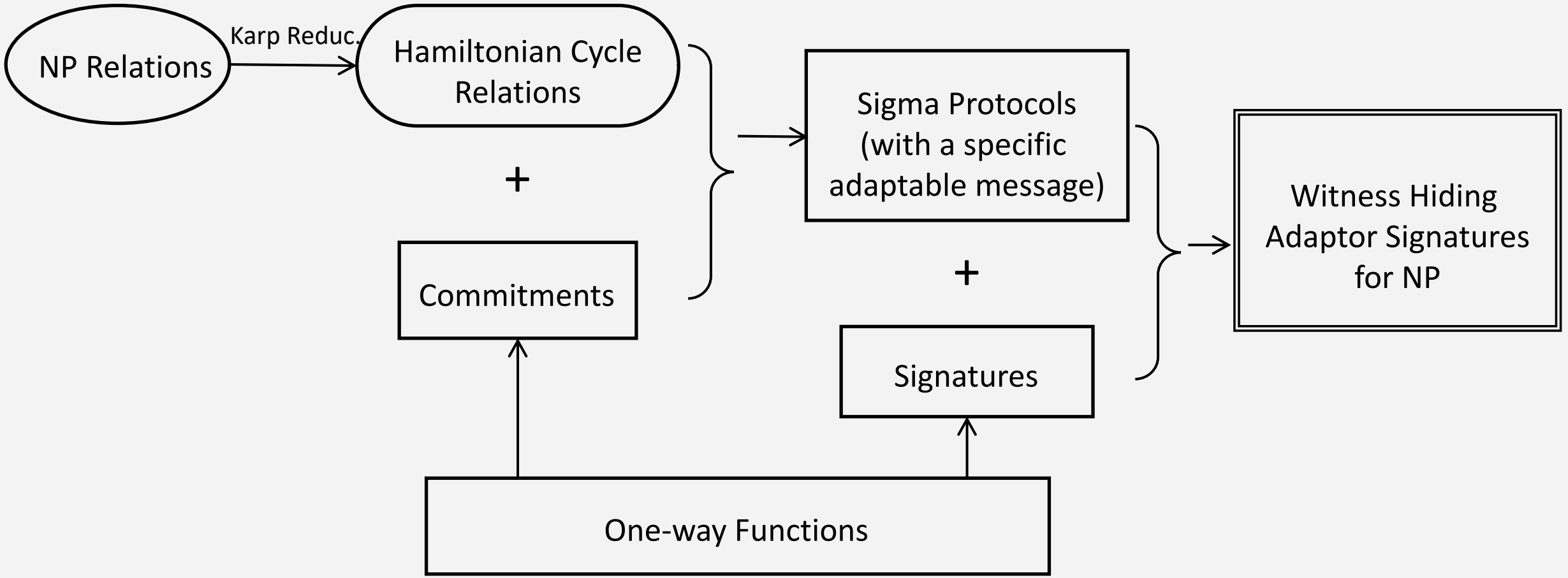
- With H and $(cmt, ch = 0, rsp)$, cmt can be opened to an other challenge $ch = 1$

From Sigma Protocol to AS

- ✓ the Hamilton cycle problem is NP-complete

- ✓ Due to Karp reduction, any NP relation R can be transferred into a Sigma protocol

Framework of AS



Conclusion

New security notion (witness hiding)

Construction of witness-hiding AS for NP

One-way functions imply witness hiding AS for NP

References

- [AEE+21] Aumayr, L., Ersoy, O., Erwig, A., Faust, S., Hostá kovᡠ, K., Maffei, M., Moreno- Sanchez, P., Riahi, S.: Generalized channels from limited blockchain scripts and adaptor signatures. In: ASIACRYPT 2021.
- [TZC22] Tu, B., Zhang, M., Yu, C.: Efficient ecdsa-based adaptor signature for batched atomic swaps. In: ISC 2022.
- [EEE20] Esgin, M.F., Ersoy, O., Erkin, Z.: Post-quantum adaptor signatures and pay- ment channel networks. In: ESORICS 2020.
- [TMM21] Tairi, E., Moreno-Sanchez, P., Maffei, M.: Post-quantum adaptor signature for privacy-preserving off-chain payments. In: FC 2021.
- [KH22] Klamti, J.B., Hasan, M.A.: Post-quantum two-party adaptor signature based on coding theory. Cryptogr. 6(1), 6 (2022).
- [EFH+21] Erwig, A., Faust, S., Hostá kovᡠ, K., Maitra, M., Riahi, S.: Two-party adaptor signatures from identification schemes. In: PKC 2021.
- [DOY22] Dai, W., Okamoto, T., Yamamoto, G.: Stronger security and generic construc- tions for adaptor signatures. In: INDOCRYPT 2022.