Distributed Signature Scheme with Monotonic Access Pattern

Yavor Litchev
Mentor: Yu Xia
MIT PRIMES Conference
October 16 - 17, 2021

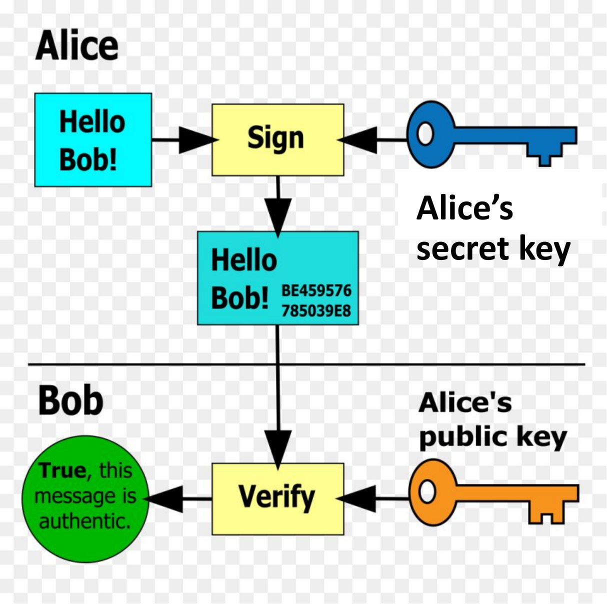
Introduction

- Digital signatures provide a practical way for a party to sign messages in an efficient manner using a private key.
- A wide variety of digital signature schemes currently exist, from RSA to El-Gamal to Schnorr.
- More recently, multi-party signature schemes have been developed.
- The proposed distributed signature scheme with monotonic access pattern allows for the modeling of complex functions.
- This results in a greater degree of access control.

What is a Digital Signature?

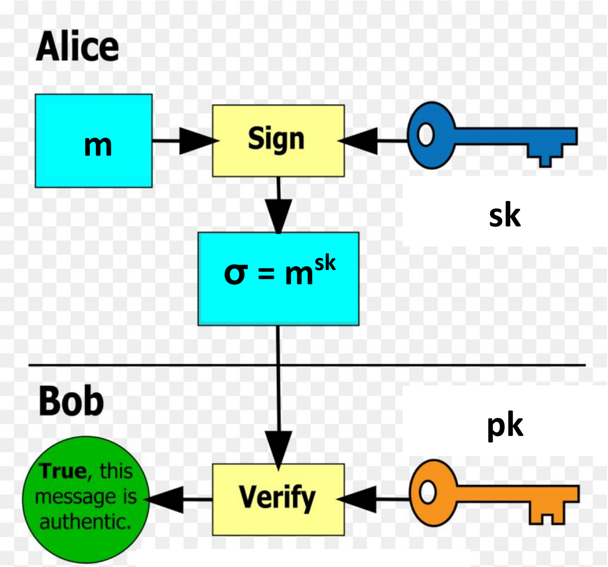
Digital Signature

- ❖ A digital signature scheme consists of 3 algorithms:
  - ➢ **K**, a key generation algorithm
  - ➢ **S**, a signature generation algorithm
  - ➢ **V**, a verification algorithm
- ❖ Alice generates pk and sk (public and secret keys respectively) using K.
- ❖ Given a message m, Alice encrypts it $\sigma = S(m, sk)$.
- ❖ Alice sends Bob σ, m, and pk, where pk is a public key.



Boneh–Lynn–Shacham (BLS) Signature Scheme

- Bilinear map: $(G_1 \times G_2 \rightarrow G_3)$ $e(a^x, b^y) = e(a,b)^{xy}$
- The BLS signature scheme is comprised of three algorithms (K, S, V):
  - **K:** Prime p and generator g are chosen. sk is sampled and $pk = g^{sk}$
  - **S:** $\sigma = m^{sk}$ is publicized
  - **V:** $e(\sigma, g) = e(m, g^{sk})$. (Evaluates to $e(m, g)^{sk}$)
- Key Homomorphism: $\sigma_1 * \sigma_2 = m^{sk_1} * m^{sk_2} = m^{sk_1+sk_2}$

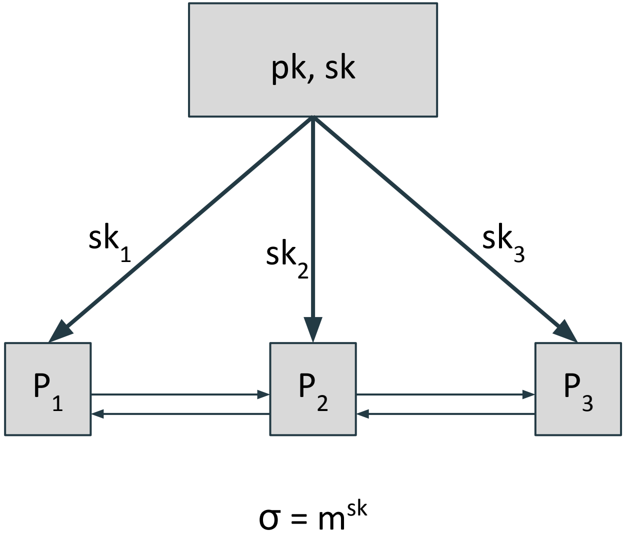


$e(\sigma, g) = e(m, g^{sk})$

What is a Distributed Signature Scheme?

Distributed Signature Scheme

- Generalized construct for a signature scheme with multiple participants
- Access structure: A defines qualified subsets
- K: pk and sk are generated, then distribute sk_1, sk_2, … sk_n for parties P_1, P_2, …. P_n.
- S: A qualifying subset for access structure A collaborate with their respective secret keys, and reconstruct $\sigma = m^{sk}$.
- V: The verification process is commenced with the public key pk on m and σ.



Monotonic Signature Scheme

Monotonic Function Access Structure

- Unate function: A boolean function $f(x_1, x_2, \ldots x_n)$ is unate if for any x_i:

  $$f(x_1, x_2 \ldots x_{i-1}, 1, x_{i+1}, \ldots x_n) \geq f(x_1, x_2 \ldots x_{i-1}, 0, x_{i+1}, \ldots x_n)$$

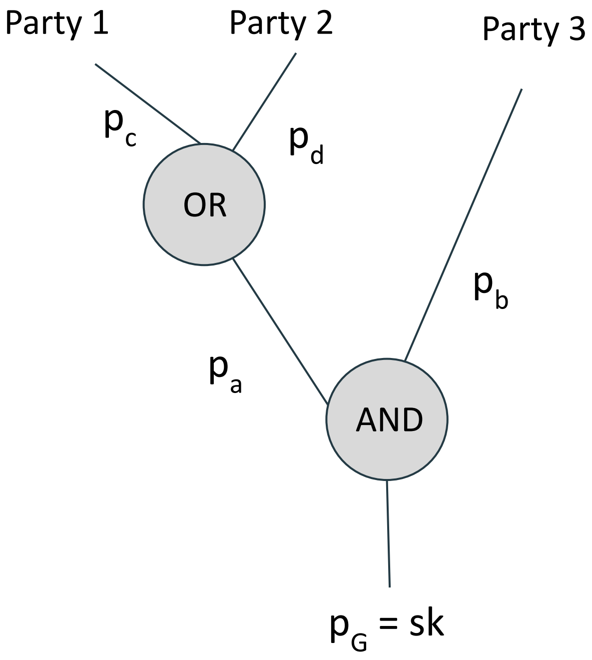
  Crucially, it can be generated with only AND, OR, and FANOUT (replication) gates.

- Monotone access structure: An access structure A such that if set B is qualified, then sets containing B with additional elements are also qualified. We form a bijective correspondence:

  $$I \in A \iff f(I) = 1$$

Overview of Monotone Signature Scheme

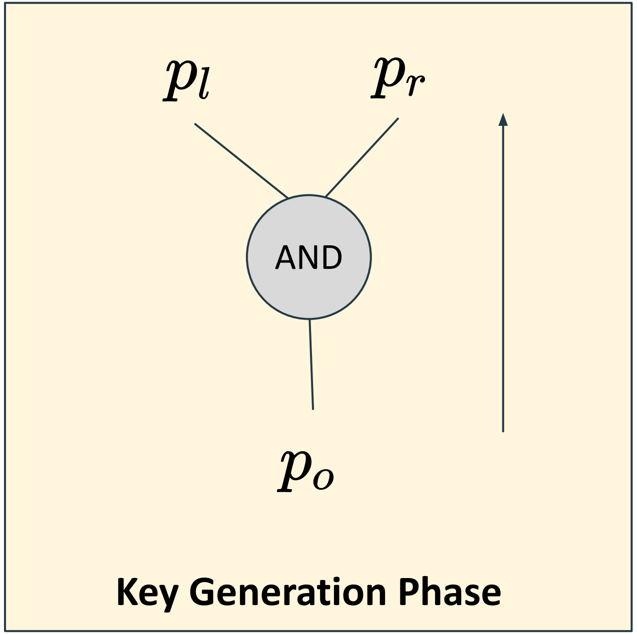
- A BLS instance is created.
- A circuit (analogous to a garbled circuit) is used to generate secret keys for each party.
- Using the same circuit, a joint signature may be generated.
- **K:** pk and sk are created from a BLS instance. sk is then assigned to the “bottom” of the circuit, party keys are generated by traveling “up” the circuit.
- **S:** Given a qualifying subset, each party generates their partial signature, and they are recombined by traversing down the same circuit.
- **V:** The signature is compared with the grandmaster public key using a bilinear map.

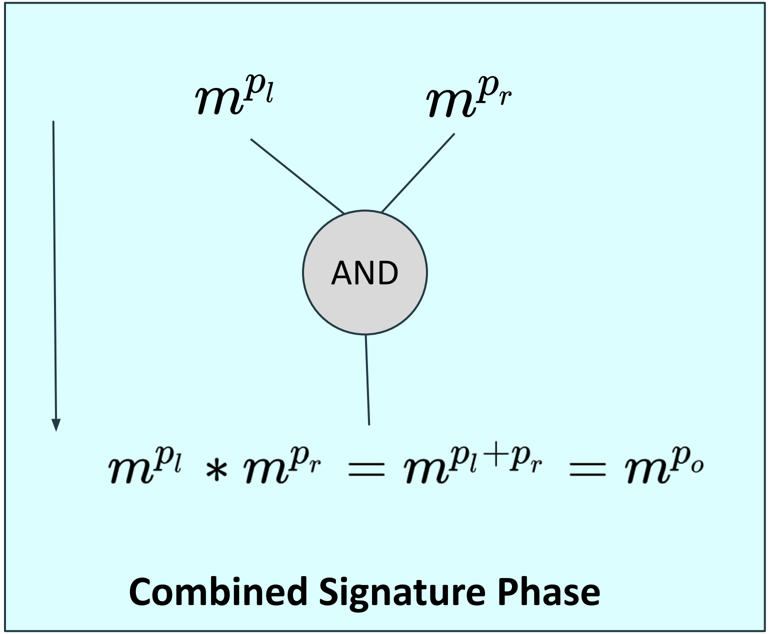


AND Gate

K: We choose private keys p_l and p_r such that $p_l + p_r = p_o$, and they are passed up the circuit.

S: The gate outputs the product of the two input signatures.

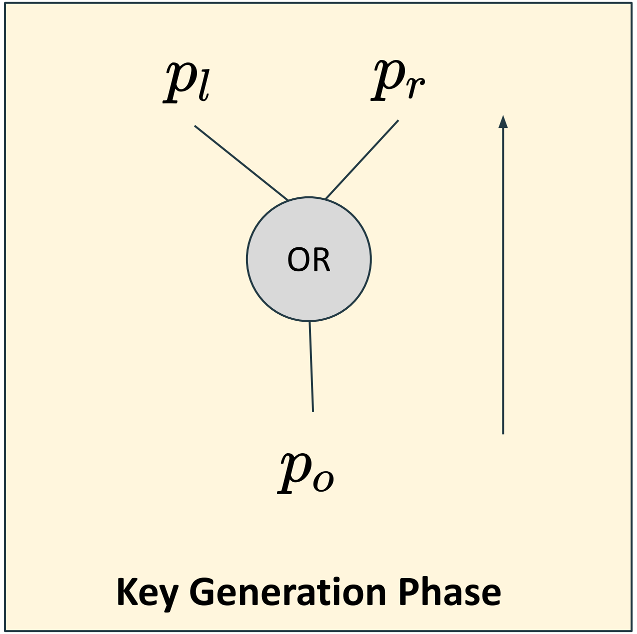


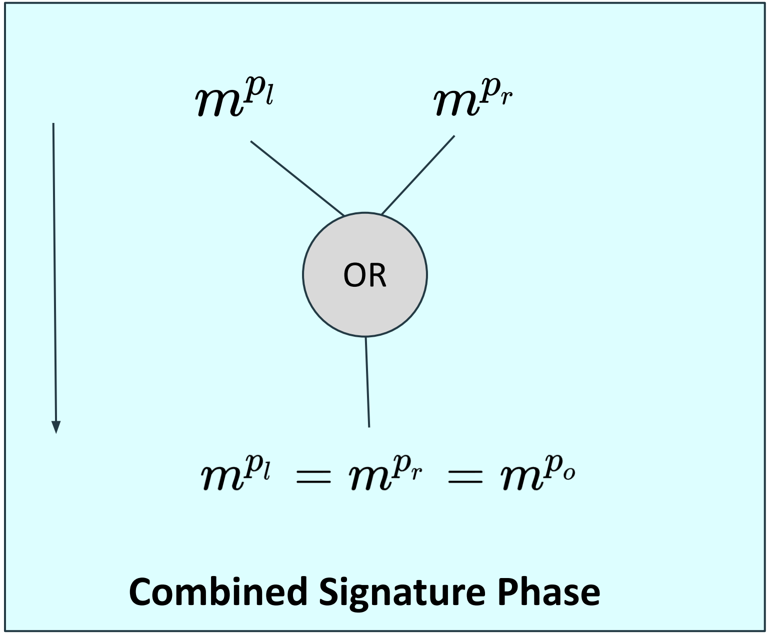


OR Gate

K: we simply set $p_l = p_r = p_o$ and pass the keys up the circuit.

S: We choose either signature, and set the output signature equal to it.

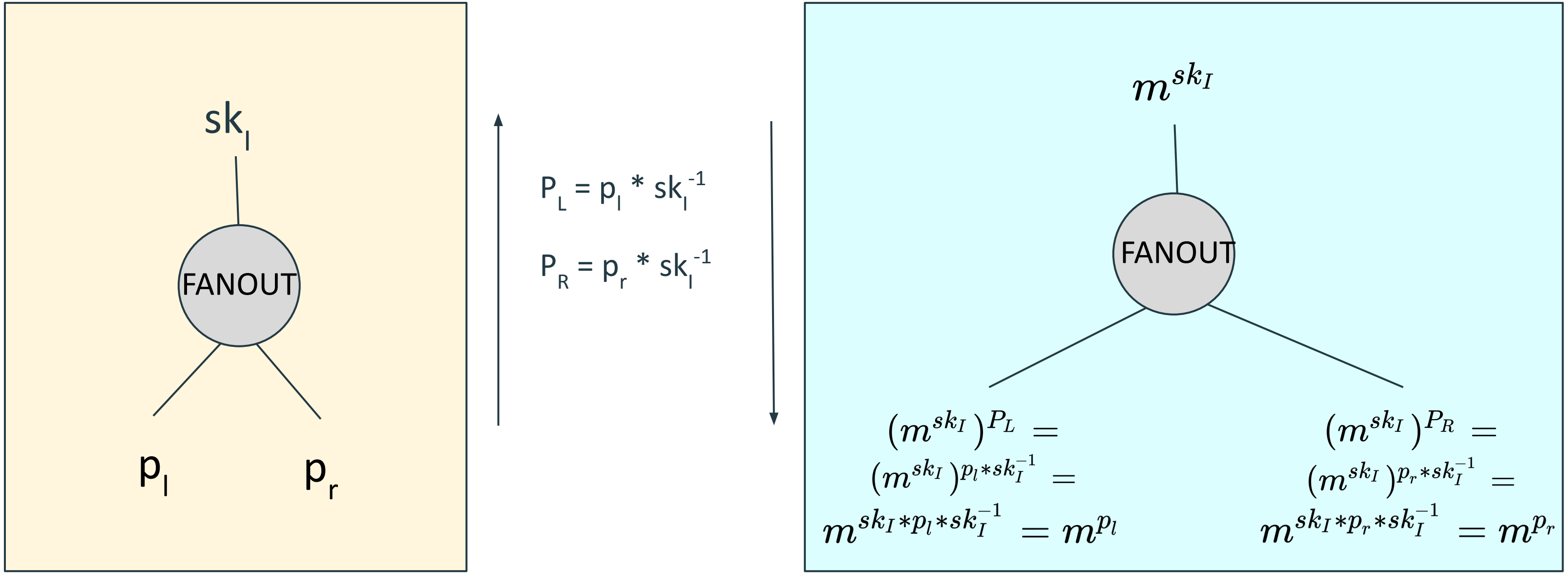




FANOUT Gate

K: We produce a random value sk_I as the secret key for the input wire, and publicize two variables $P_L = p_l * sk_I^{-1}$ and $P_R = p_r * sk_I^{-1}$.

S: We exponentiate the input signature by each of the respective public variables.



Limitations and Problems

Leakage from FANOUT Gates

- For every FANOUT gate we publish two public values $P_L = p_l * sk_l^{-1}$ and $P_R = p_r * sk_l^{-1}$.
- However, $P_L * P_R^{-1} = p_l * p_r^{-1}$ may be computed.
- Can potentially be mitigated with key-length doubling, or the use of additional secret encryption keys.

Conclusion

Applications

- Threshold signature schemes are limited in their capacity to model complex access structures.
- The proposed scheme allows to model more sophisticated access structures.
- In addition to signing documents, the signature scheme can be used for hierarchical access control (ex. entering an office building, file access in a server, etc).

Future Research

- Utilization of randomized signature schemes for additional security (e.g. Schorr).
- Solving of existing problems such as Dolev-Strong.
- Reduce number of published values in FANOUT gates.

Acknowledgements

I would like to thank:

- My mentor Yu Xia
- The PRIMES program
- My family

THE END