

NC STATE UNIVERSITY Computer Science

CSC 774 Advanced Network Security

Topic 4.2 BiBa

Dr. Peng Ning CSC 774 Adv. Net. Security 1

Overview

- BiBa stands for “Bins and Balls”
 - Use one-way functions without trapdoors (e.g., hash functions)
- BiBa signature scheme
- BiBa broadcast authentication protocol

NC STATE UNIVERSITY Computer Science Dr. Peng Ning CSC 774 Adv. Net. Security 2

BiBa Signature Scheme

- Precompute of SEALs
 - SEAL: SElf Authenticating vaLues
- Signature generation
 - Exploit SEALs and the difficulty of finding collisions under hash functions
- Signature verification
 - Verify SEAL
 - Verify collisions

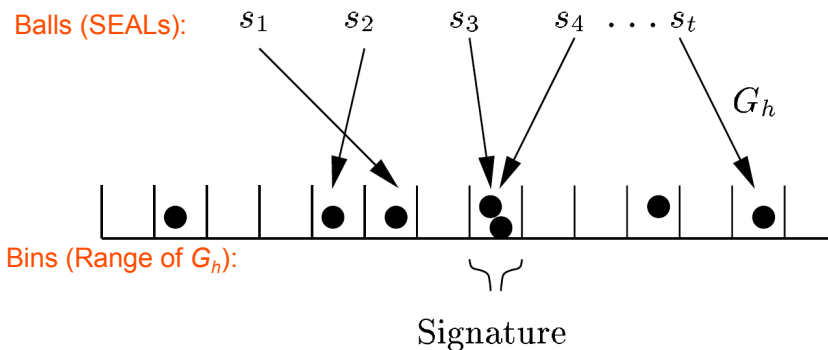
SEAL

- Each SEAL is randomly generated
- Given a SEAL s , the signer computes $f_s = F_s(0)$, where F_s is a PRF
 - f_s is the **commitment** to s
 - f_s is authenticated to all possible verifiers (e.g., through a RSA signature or pre-distribution)
- In BiBa, the signer has t pre-computed SEALs
 - SEALs: s_1, s_2, \dots, s_t
 - All SEALs are authenticated to all verifiers

BiBa Signature: Intuition

- Sign message m
 - Compute hash $h = H(m)$, where H is a hash function
 - Consider a **hash function family** G_h , whose range is $0, n-1$
 - Example: $G_l(x) = G(x|l)$, where G is SHA1
 - Compute G_h for all SEALS s_1, \dots, s_t
 - That is, $G_h(s_1), G_h(s_2), \dots, G_h(s_t)$
 - Look for a **2-way collision** of SEALS
 - $G_h(s_i) = G_h(s_j)$ with $s_i \neq s_j$
 - The pair $\langle s_i, s_j \rangle$ forms the signature
- Signature verification
 - Compute hash $h = H(m)$
 - Verify $s_i \neq s_j$ and $G_h(s_i) = G_h(s_j)$

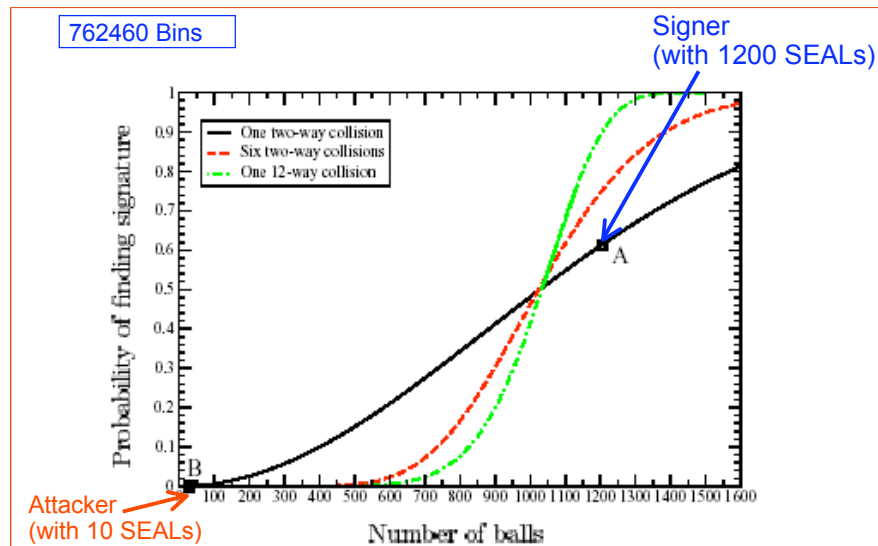
Basic BiBa Scheme



Security of BiBa Signature

- Security comes from
 - The difficulty of finding k -way collisions for one-way functions
 - The asymmetric property that the signer has more SEALs than the adversary
 - Signer can easily generate the BiBa signatures with high probability while adversary can't.
- Exploits the birthday paradox
 - Probability that there is at least one collision of the hashes of t random messages is approximately
 - $1 - e^{-t(t-1)/2N}$, where N is range of hash function.

Security of BiBa Signature (Cont'd)



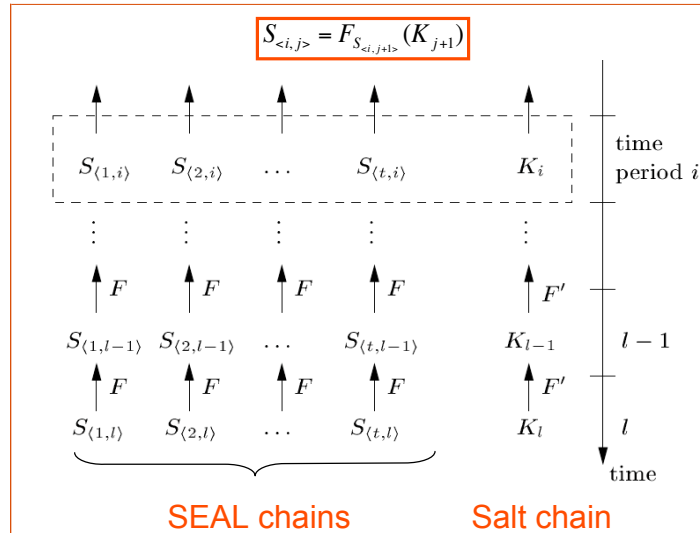
BiBa Signature Scheme

- Basic scheme
 - Signer is not guaranteed to find a signature
- BiBa Signature
 - Sign message m
 - $h=H(m|c)$, where c is a counter starting from 0
 - c is incremented if no signature is found
 - Compute G_h for all SEALs s_1, \dots, s_t
 - Look for a k -way collision of SEALs
 - Verify signature
 - Verify the k SEALs are distinct
 - Verify that they have the same image

BiBa Broadcast Authentication Protocol

- Sender needs to authenticate potentially infinite stream of messages
- Sender can only disclose a small number of SEALs before attacker would have enough to forge signature
 - Limit the number of messages that can be signed
- Solution
 - SEAL chains
 - Combination of SEALs and TESLA

SEAL Chains

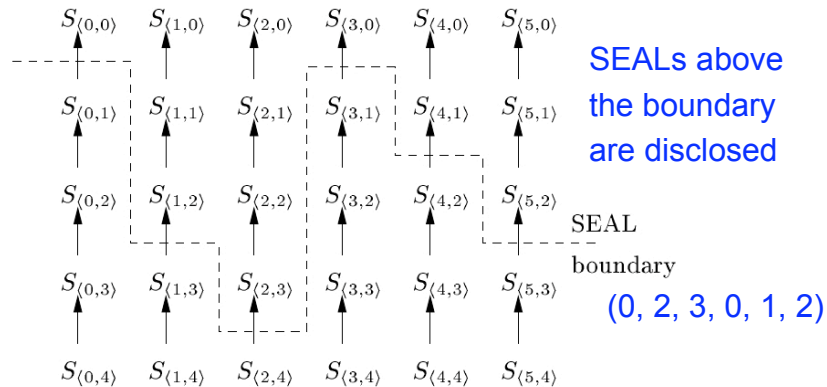


Limitation of BiBa Broadcast Authentication

- High receiver computation overhead
 - Most of the SEALS are not used
 - To authenticate a SEAL, each receiver needs to recompute many SEALS in a one-way SEAL chain

Extension A

- SEAL boundary



- If attacker slows down the traffic to the receivers, ...
- Packet losses

Extension B

- To tolerate packet losses
 - Add SEAL boundary information to packets
 - More communication overhead, but also more robust
- Receivers still need to know the sending rate
 - Why?