



Universität Hamburg

Using Cryptographically Generated SIP-URIs to Protect the Integrity of Content in P2P-SIP

Jan Seedorf

University of Hamburg, Germany

seedorf@informatik.uni-hamburg.de

**Third Annual VoIP Security Workshop
June 1st & 2nd, 2006, Berlin, Germany**



**Department Informatik
SVS – Security in Distributed Systems**



During the next 25 minutes I would like to show you:

- **How we can statically bind a public/private key pair to a SIP-URI**
- **Why this helps protecting SIP-registrations in scenarios with a lack of trust**
- **How this can be used in P2P-SIP**



- I. Why use Self-Certifying Identities?**
- II. Cryptographically Generated SIP-URIs**
- III. Using Cryptographically Generated SIP-URIs in P2P-SIP**
- IV. Benefits vs. Drawbacks**
- V. Conclusion**



SIP-URIs

- Enable mobility in SIP
- e.g. user@domain
- Identity in SIP

Security of Registrations

- Depends on trust in the registrar (& intermediate entities)

Secure Identities

- Start with a public key as the identity in the system
- Can we statically bind an asymmetric key pair with a SIP-URI?

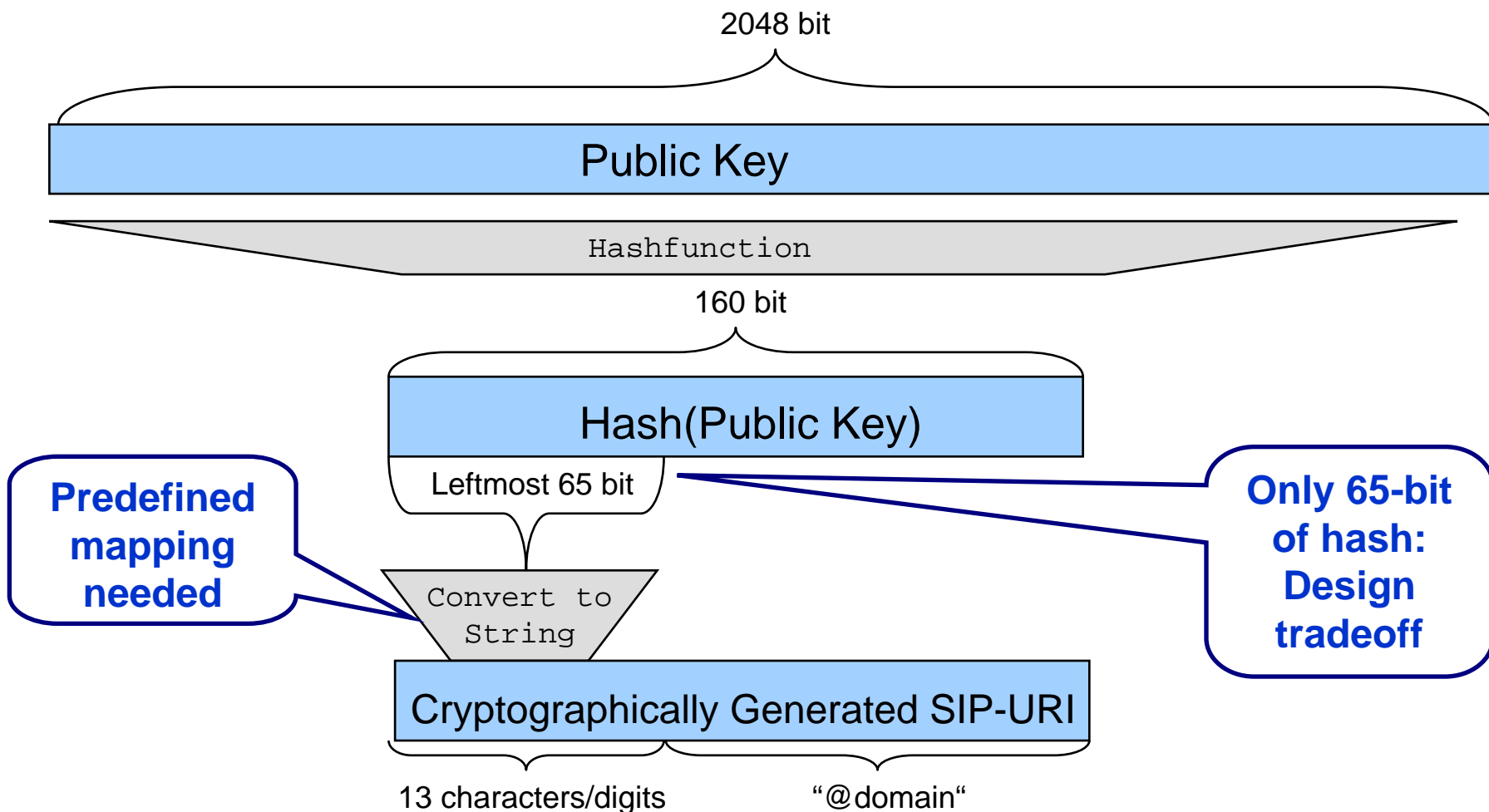


Self-certifying identities

- An identity where ownership of the identity can be verified without relying on a trusted third party

How can this be done?

- Start with a private/public key pair
- Represent the identity as the hash of the public key
- Sign the identity with the corresponding private key and append public key
- Anybody can verify the signature by
 - a) Checking that the hash of the public key is the identity
 - b) Verifying the signature with the public key



Private/Public Key and SIP-URI are securely bound to each other!



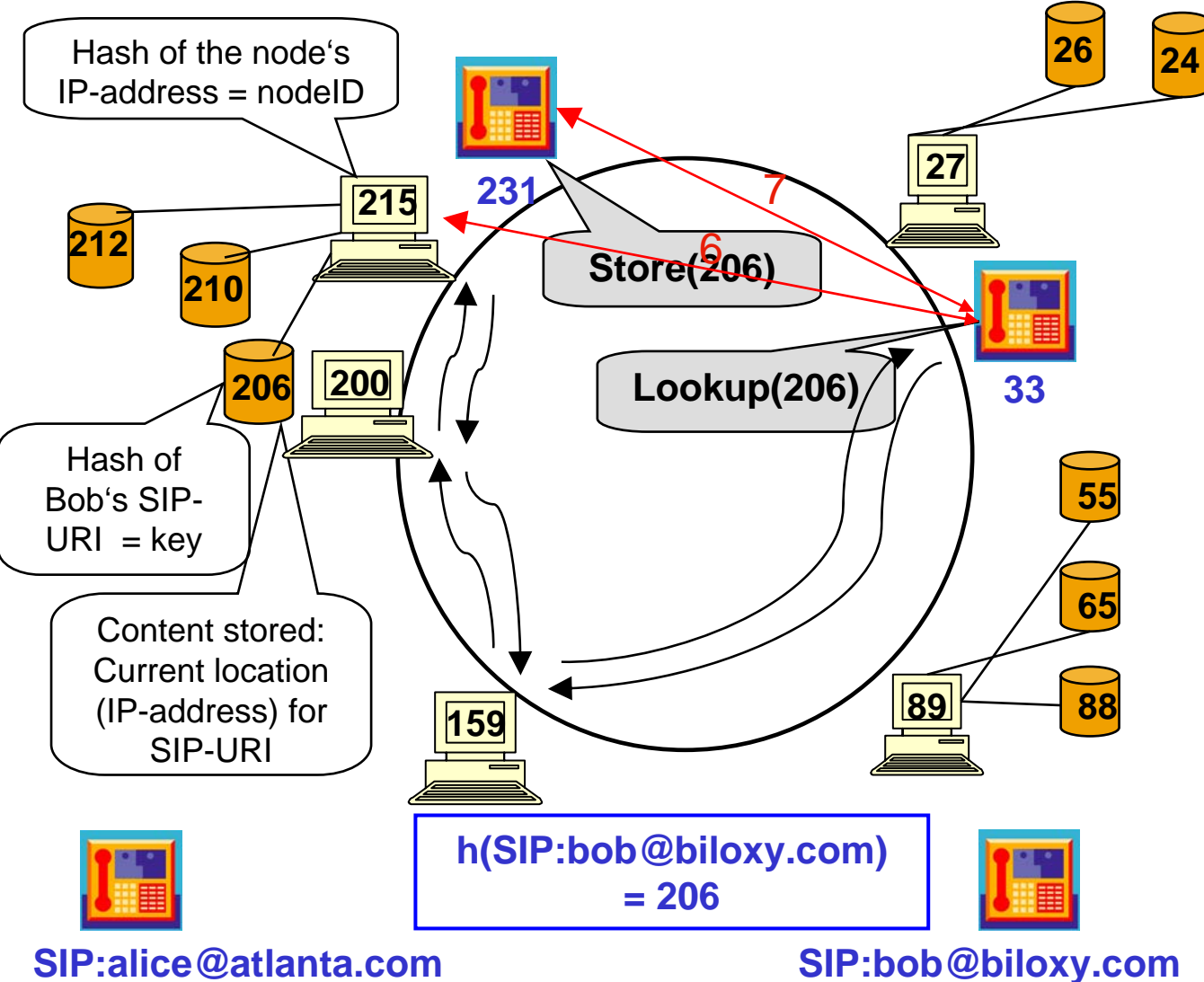
What is P2P-SIP?

- Using a peer-to-peer network as a substrate for SIP user registration and location lookup

A scenario where we do not have any trust at all in the registrar, because

- it is assigned arbitrary to the user
- it changes frequently

=> no pre-established trust between registrar and user possible



Distributed Hash Table (DHT) offers:
Store(key)
Lookup(key)

- (1) Bob's node joins the DHT
- (2) Alice's node joins the DHT
- (3) Bob registers his URI with the DHT
- (4) Alice wants to call Bob
- (5) DHT delivers the node (+IP-address) responsible for Bob's URI to Alice (node 215)
- (6) Alice contacts node 215 to get Bob's IP-address (without using the overlay)
- (7) Alice and Bob negotiate parameters and set up their session directly (without using the overlay)

How to trust node 215?



P2P Paradigm introduces new security problems

- **No central authority in the network**
 - ◆ **No trust in other nodes in the network**
- **Distributed Hash Table is highly dynamic**
 - ◆ **Node responsible for storing location of a SIP-URI changes frequently**
- **Adversary nodes can:**
 - ◆ **Spoof identity**
 - ◆ **Falsify messages in the overlay**
 - ◆ **Insert false messages in the overlay**
 - ◆ **...**



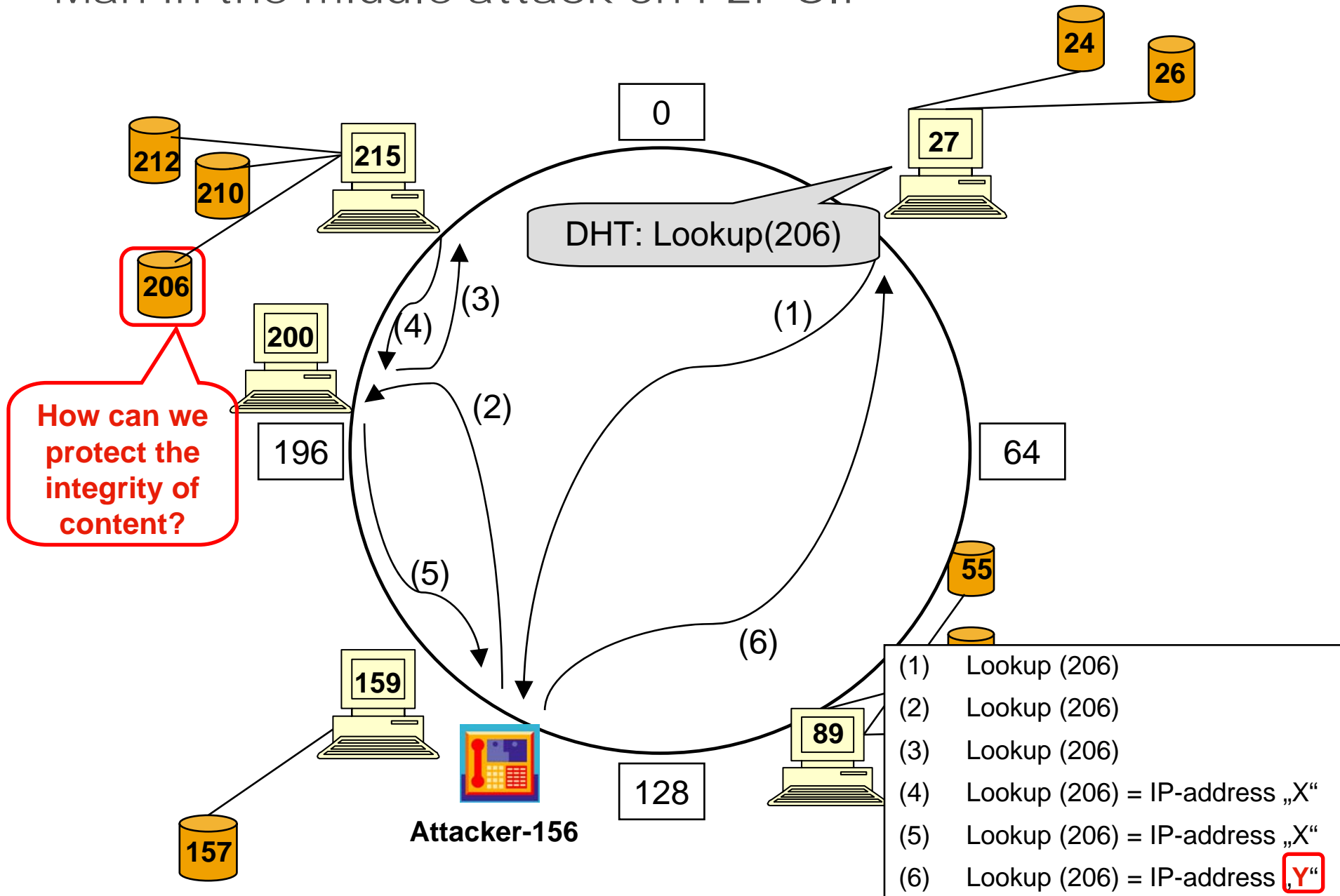
Focus of this talk

- Protecting the integrity of content stored in the overlay

Why must the integrity of content be protected?

- Content stored in P2P-SIP overlay
 - ◆ Binding of location (IP-address/port) and SIP-URI
- SIP-URI
 - ◆ Identity used in the system
 - ◆ Impersonation of this identity needs to be prevented
 - ◆ Otherwise, single SIP-URIs can be attacked

Man-in-the-middle attack on P2P SIP





Adding a central authority

- Takes away most benefits of P2P computing
 - ◆ Not scalable
 - ◆ Single point of failure/attack

Using a distributed reputation management system to build “trust”

- Gain reputation for what?

Self-certifying identities

- e.g. Cryptographically Generated SIP-URIs



Registering a SIP-URI

- Sign current location with private key
- Store in overlay:
[URI , location, **signed location, public key**]

Verifying

1. Lookup(key) =
[URI , location, **signed location, public key**]
2. Check that the hash of the public key is the first part of the SIP-URI
3. Verify the signature of the location with the public key



No central authority

- Scalable solution (true P2P)

Verification possible at all routing hops

- Not only the requesting node can do the verification
=> Any node can detect altered messages

Independent of routing strategy or overlay

- P2P-SIP is in an early stage, overlay protocol may change in the future

Compatible with any (existing) SIP entity

- Cryptography is encoded solely in the SIP-URI



Readability of SIP-URIs

- e.g. h6k6spog43kl2@your-domain.com

Attacks on the hash function

- Collision resistance
- Second pre-image resistance

Denial-of-Service Attacks

- Added cryptography consumes performance

Reliable Association of SIP-URI and User

- Out-of-overlay
- Only once per callee/SIP-URI
- Examples
 - ◆ Web-of-trust
 - ◆ https website



- **P2P-SIP is in an early stage, not secure yet**
- **Self-Certifying SIP-URIs are one option to protect the integrity of content in such a network**
- **Such a solution enables verification of location-bindings stored in the overlay**
 - **at any place in the overlay**
 - **without a central authority as part of the overlay**
 - **independent of the distributed hash table being used**
 - **compatible with any existing SIP entity**