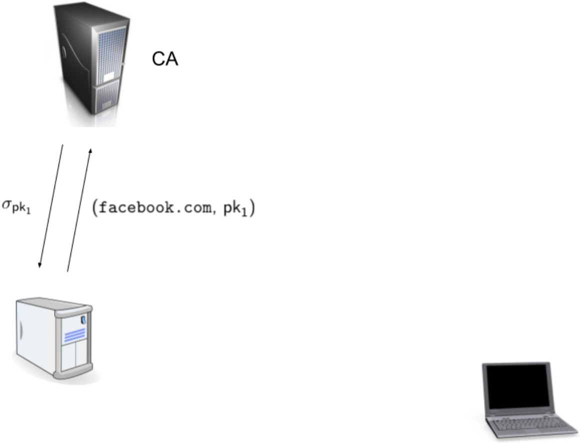
Lattice-based DAPS and Generalizations

Dan Boneh, Sam Kim, Valeria Nikolaenko

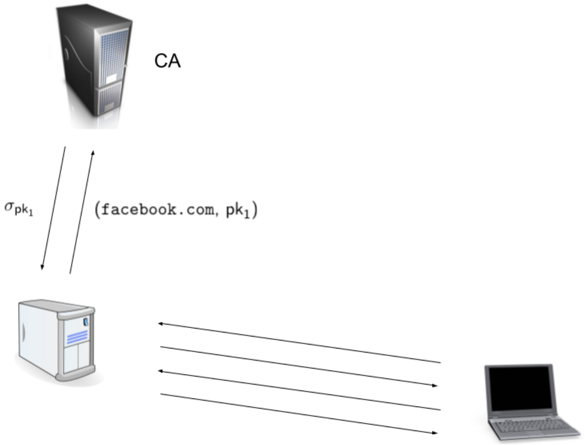
Stanford University

July 11, 2017

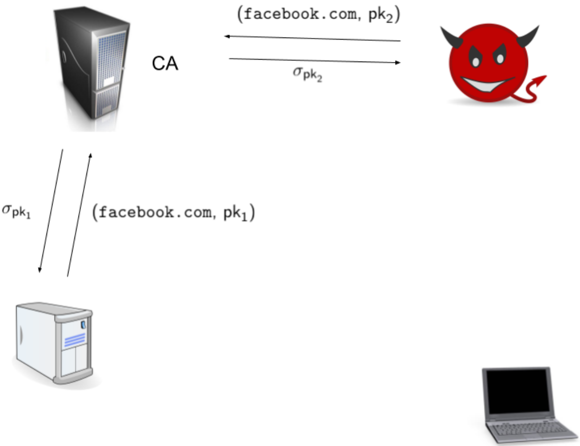
Certificate Authorities



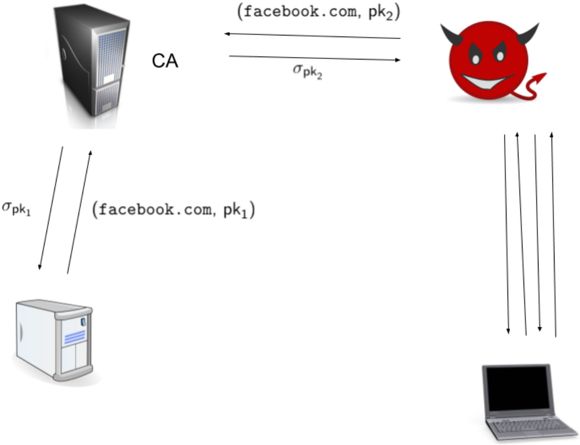
Certificate Authorities



Certificate Authorities



Certificate Authorities



Signatures

- For many scenarios, signers are **trusted** to make **unique bindings**
  - Certificate Authorities
  - Time Stamping Authorities

Signatures

- For many scenarios, signers are **trusted** to make **unique bindings**
  - Certificate Authorities
  - Time Stamping Authorities
- But traditional digital signatures impose no **uniqueness condition**

Signatures

- For many scenarios, signers are **trusted** to make **unique bindings**
  - Certificate Authorities
  - Time Stamping Authorities
- But traditional digital signatures impose no **uniqueness condition**
- Often times, signers are **coerced** into making fake certificates (double-signing)

Signatures

- For many scenarios, signers are **trusted** to make **unique bindings**
  - Certificate Authorities
  - Time Stamping Authorities
- But traditional digital signatures impose no **uniqueness condition**
- Often times, signers are **coerced** into making fake certificates (double-signing)
- What can we do in these type of situations?

Signatures

- For many scenarios, signers are **trusted** to make **unique bindings**
  - Certificate Authorities
  - Time Stamping Authorities
- But traditional digital signatures impose no **uniqueness condition**
- Often times, signers are **coerced** into making fake certificates (double-signing)
- What can we do in these type of situations?
- Are there mechanisms to really force the CA to act honestly even in the face of coercion?

Double Signing

- There are mechanisms to **detect** when a CA issues a fake certificate
  - Certificate Transparency (CT) [LLK15]
  - CONIKS [MBB+15]

Double Signing

- There are mechanisms to **detect** when a CA issues a fake certificate
  - Certificate Transparency (CT) [LLK15]
  - CONIKS [MBB+15]
- However, often times punishment not so severe
  - A period of bad publicity

Double Signing

- There are mechanisms to **detect** when a CA issues a fake certificate
  - Certificate Transparency (CT) [LLK15]
  - CONIKS [MBB+15]
- However, often times punishment not so severe
  - A period of bad publicity
- Consequences not severe enough to prevent **legal coercion**

Double Signing

- There are mechanisms to **detect** when a CA issues a fake certificate
  - Certificate Transparency (CT) [LLK15]
  - CONIKS [MBB+15]
- However, often times punishment not so severe
  - A period of bad publicity
- Consequences not severe enough to prevent **legal coercion**
- Can we make the consequences more severe such that the CA can use it as an argument against coercion?

DAPS

- **Double Authentication Preventing Signatures** (DAPS) [PS14]

DAPS

- **Double Authentication Preventing Signatures** (DAPS) [PS14]
- Message of them form $(\mathsf{subj}, \mathsf{payload})$

DAPS

- **Double Authentication Preventing Signatures** (DAPS) [PS14]
- Message of them form $(\mathsf{subj}, \mathsf{payload})$
- Signatures of $(\mathsf{subj}, \mathsf{payload}_1)$, $(\mathsf{subj}, \mathsf{payload}_2)$ leaks signing key

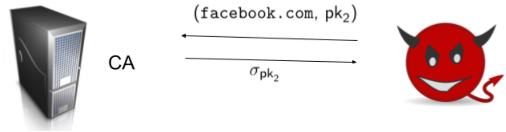
DAPS

- **Double Authentication Preventing Signatures** (DAPS) [PS14]
- Message of them form $(\mathsf{subj}, \mathsf{payload})$
- Signatures of $(\mathsf{subj}, \mathsf{payload}_1)$, $(\mathsf{subj}, \mathsf{payload}_2)$ leaks signing key
- CA uses as **self-enforcement**

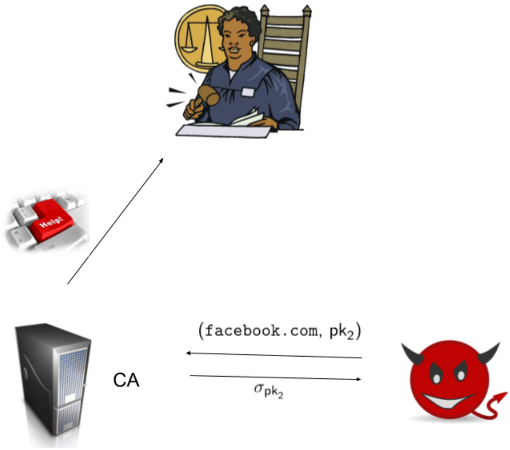
DAPS

- **Double Authentication Preventing Signatures** (DAPS) [PS14]
- Message of them form $(\mathsf{subj}, \mathsf{payload})$
- Signatures of $(\mathsf{subj}, \mathsf{payload}_1)$, $(\mathsf{subj}, \mathsf{payload}_2)$ leaks signing key
- CA uses as **self-enforcement**
- CA will use DAPS as a justification to resist coercion

Legal Coercion



Legal Coercion



Legal Coercion

Right Notion?

Q : What if Facebook happens to accidentally lose its certificate?

Right Notion?

Q : What if Facebook happens to accidentally lose its certificate?

A : Use short-lived certificates

Right Notion?

Q : What if Facebook happens to accidentally lose its certificate?

A : Use short-lived certificates

Q : What if agency simply coerces another CA to issue a certificate for facebook.com?

Right Notion?

Q : What if Facebook happens to accidentally lose its certificate?

A : Use short-lived certificates

Q : What if agency simply coerces another CA to issue a certificate for facebook.com?

A : Use certificate pinning

Right Notion?

Q : What if Facebook happens to accidentally lose its certificate?

A : Use short-lived certificates

Q : What if agency simply coerces another CA to issue a certificate for facebook.com?

A : Use certificate pinning

Q : What if Facebook wishes to use a different certificate for each server?

Right Notion?

Q : What if Facebook happens to accidentally lose its certificate?

A : Use short-lived certificates

Q : What if agency simply coerces another CA to issue a certificate for facebook.com?

A : Use certificate pinning

Q : What if Facebook wishes to use a different certificate for each server?

A : Use intermediate CA's

Right Notion?

Q : What if Facebook happens to accidentally lose its certificate?

A : Use short-lived certificates

Q : What if agency simply coerces another CA to issue a certificate for facebook.com?

A : Use certificate pinning

Q : What if Facebook wishes to use a different certificate for each server?

A : Use intermediate CA's

There are other holes in the argument (but that is not the point!)

DAPS Formulation

- $\mathsf{Setup} \to (\mathsf{sk}, \mathsf{vk})$
- $\mathsf{Sign}(\mathsf{sk}, \mathsf{msg}) \to \sigma$
- $\mathsf{Verify}(\mathsf{vk}, \mathsf{msg}, \sigma) \to 0/1$

DAPS Formulation

- $\mathsf{Setup} \to (\mathsf{sk}, \mathsf{vk})$
- $\mathsf{Sign}(\mathsf{sk}, (\mathsf{subj}, \mathsf{payload})) \to \sigma$
- $\mathsf{Verify}(\mathsf{vk}, \mathsf{msg}, \sigma) \to 0/1$
- $\mathsf{Extract}((\mathsf{subj}, \mathsf{payload}_1), \sigma_1, (\mathsf{subj}, \mathsf{payload}_2), \sigma_2) \to \mathsf{sk}$

Results

- Previously, [PS14] construct DAPS from the hardness of **factoring**

Results

- Previously, [PS14] construct DAPS from the hardness of **factoring**
- **This Work**:
  - Construct DAPS from lattices (SIS)
  - Provide generalization of DAPS
  - Extend to multi-authority setting

SIS

Let n, m, q, β be appropriately chosen positive integers.

Short Integer Solutions (SIS) Problem

Given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find *short* a nonzero $\mathbf{u} \in \mathbb{Z}^m$ such that $\mathbf{A} \cdot \mathbf{u} = \mathbf{0}$.

SIS

Let n, m, q, β be appropriately chosen positive integers.

Inhomogeneous SIS Problem

Given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, and a vector $\mathbf{v} \in \mathbb{Z}_q^n$, find a *short* nonzero $\mathbf{u} \in \mathbb{Z}^m$ such that $\mathbf{A} \cdot \mathbf{u} = \mathbf{v}$.

SIS

Let n, m, q, β be appropriately chosen positive integers.

Inhomogeneous SIS Problem

Given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, and a vector $\mathbf{v} \in \mathbb{Z}_q^n$, find a *short* nonzero $\mathbf{u} \in \mathbb{Z}^m$ such that $\mathbf{A} \cdot \mathbf{u} = \mathbf{v}$.

Nice properties:

- Solving SIS results in solving worst-case lattice problems!
- Possible to generate $\mathbf{A}$ with a trapdoor $\mathbf{td}$ such that SIS easy to solve

GPV Signatures

Signature scheme using hash-and-sign [GPV08]

- $\mathsf{vk} = \mathbf{A} \qquad \mathsf{sk} = \mathbf{td}$
- $\mathsf{Sign}(\mathsf{sk}, \mathsf{msg})$: Hash $\mathbf{v} = H(\mathsf{msg}) \in \mathbb{Z}_q^n$ and compute $\sigma = \mathbf{u}$ such that $\mathbf{A} \cdot \mathbf{u} = \mathbf{v}$
- $\mathsf{Verify}(\mathsf{vk}, \mathsf{msg}, \sigma)$: Verify that $\mathbf{A} \cdot \mathbf{u} = \mathbf{v}$ and $|\mathbf{u}|$ short.

Gadget trapdoors

Let $\mathbf{G}$ be a special "gadget matrix" where SIS easy
(Find short $\mathbf{u}$ such that $\mathbf{G} \cdot \mathbf{u} = \mathbf{v}$)

Gadget trapdoors

Let $\mathbf{G}$ be a special "gadget matrix" where SIS easy
(Find short $\mathbf{u}$ such that $\mathbf{G} \cdot \mathbf{u} = \mathbf{v}$)

Trapdoor **td** for $\mathbf{A}$ defined as a **short**, **full-rank** matrix $\mathbf{R}$ such that $\mathbf{A} \cdot \mathbf{R} = \mathbf{H} \cdot \mathbf{G}$ for any invertible matrix $\mathbf{H} \in \mathbb{Z}_q^{n \times n}$.

Gadget trapdoors

Let $\mathbf{G}$ be a special "gadget matrix" where SIS easy
(Find short $\mathbf{u}$ such that $\mathbf{G} \cdot \mathbf{u} = \mathbf{v}$)

Trapdoor **td** for $\mathbf{A}$ defined as a **short**, **full-rank** matrix $\mathbf{R}$ such that $\mathbf{A} \cdot \mathbf{R} = \mathbf{H} \cdot \mathbf{G}$ for any invertible matrix $\mathbf{H} \in \mathbb{Z}_q^{n \times n}$.

To sample pre-image $\mathbf{u}$:

1. Sample short $\tilde{\mathbf{u}}$ such that $\mathbf{G} \cdot \tilde{\mathbf{u}} = \mathbf{v}$
2. Let $\mathbf{u} = \mathbf{R} \cdot \tilde{\mathbf{u}}$. Then

$$\mathbf{A}\mathbf{u} = \mathbf{A} \cdot \mathbf{R} \cdot \tilde{\mathbf{u}} = \mathbf{v}$$

In the real scheme, must take care of distributional issues

FRD Encodings

Full-Rank Difference (FRD) encoding:

Encoding function $H_{\mathsf{FRD}} : \mathbb{Z}_q^n \to \mathsf{GL}(\mathbb{Z}_q^{n \times n})$

- For any two distinct vectors $\mathbf{u}, \mathbf{v}$, the matrix $H_{\mathsf{FRD}}(\mathbf{u}) - H_{\mathsf{FRD}}(\mathbf{v})$ is full rank

DAPS Construction

Fix a hash function H and FRD encoding H_{FRD}.

- $\mathsf{vk} = \mathbf{A}, \qquad \mathsf{sk} = \mathbf{td}$
- $\mathsf{Sign}(\mathsf{sk}, (\mathsf{subj}, \mathsf{payload}))$:
  1. $\mathbf{V} = H(\mathsf{subj}) \in \mathbb{Z}_q^{n \times m}$
  2. $\mathbf{H} = H_{\mathsf{FRD}}(\mathsf{payload}) \in Z_q^{n \times n}$
  3. Let $\sigma = \mathbf{U}$ be a short matrix $\mathbf{U}$ such that $\mathbf{A} \cdot \mathbf{U} + \mathbf{H} \cdot \mathbf{G} = \mathbf{V}$
- $\mathsf{Verify}(\mathsf{vk}, (\mathsf{subj}, \mathsf{payload}), \sigma)$: Verify the relation $\mathbf{A} \cdot \mathbf{U} + \mathbf{H} \cdot \mathbf{G} = \mathbf{V}$ and check $\mathbf{U}$ short

DAPS Construction

- $\mathsf{Extract}((\mathsf{subj}, \mathsf{payload}_1), \sigma_1, (\mathsf{subj}, \mathsf{payload}_2), \sigma_2)$:
  We have two signatures $\sigma_1 = \mathbf{U}_1$, $\sigma_2 = \mathbf{U}_2$ such that

$$\mathbf{A} \cdot \mathbf{U}_1 + H_{\mathsf{FRD}}(\mathsf{payload}_1) \cdot \mathbf{G} = H(\mathsf{subj})$$

$$\mathbf{A} \cdot \mathbf{U}_2 + H_{\mathsf{FRD}}(\mathsf{payload}_2) \cdot \mathbf{G} = H(\mathsf{subj})$$

DAPS Construction

- $\mathsf{Extract}((\mathsf{subj}, \mathsf{payload}_1), \sigma_1, (\mathsf{subj}, \mathsf{payload}_2), \sigma_2)$:
  We have two signatures $\sigma_1 = \mathbf{U}_1$, $\sigma_2 = \mathbf{U}_2$ such that

$$\mathbf{A} \cdot \mathbf{U}_1 + \mathbf{H}_1 \cdot \mathbf{G} = \mathbf{V}$$

$$\mathbf{A} \cdot \mathbf{U}_2 + \mathbf{H}_2 \cdot \mathbf{G} = \mathbf{V}$$

DAPS Construction

- $\mathsf{Extract}((\mathsf{subj}, \mathsf{payload}_1), \sigma_1, (\mathsf{subj}, \mathsf{payload}_2), \sigma_2)$:
  We have two signatures $\sigma_1 = \mathbf{U}_1$, $\sigma_2 = \mathbf{U}_2$ such that

$$\mathbf{A} \cdot (\mathbf{U}_1 - \mathbf{U}_2) = (\mathbf{H}_2 - \mathbf{H}_1)\mathbf{G}$$

DAPS Construction

- Extract$((\mathsf{subj}, \mathsf{payload}_1), \sigma_1, (\mathsf{subj}, \mathsf{payload}_2), \sigma_2)$:
  We have two signatures $\sigma_1 = \mathbf{U}_1$, $\sigma_2 = \mathbf{U}_2$ such that

$$\mathbf{A} \cdot (\underbrace{\mathbf{U}_1 - \mathbf{U}_2}_{\text{short}}) = (\mathbf{H}_2 - \mathbf{H}_1)\mathbf{G}$$

DAPS Construction

- Extract$((\mathsf{subj}, \mathsf{payload}_1), \sigma_1, (\mathsf{subj}, \mathsf{payload}_2), \sigma_2)$:
  We have two signatures $\sigma_1 = \mathbf{U}_1$, $\sigma_2 = \mathbf{U}_2$ such that

$$\mathbf{A} \cdot (\mathbf{U}_1 - \mathbf{U}_2) = (\underbrace{\mathbf{H}_2 - \mathbf{H}_1}_{\text{full-rank}})\mathbf{G}$$

DAPS Construction

- $\mathsf{Extract}((\mathsf{subj}, \mathsf{payload}_1), \sigma_1, (\mathsf{subj}, \mathsf{payload}_2), \sigma_2)$:
  We have two signatures $\sigma_1 = \mathbf{U}_1$, $\sigma_2 = \mathbf{U}_2$ such that

$$\mathbf{A} \cdot (\mathbf{U}_1 - \mathbf{U}_2) = (\underbrace{\mathbf{H}_2 - \mathbf{H}_1}_{\text{full-rank}})\mathbf{G}$$

  The matrix $(\mathbf{U}_1 - \mathbf{U}_2)$ trapdoor for $\mathbf{A}$

Predicate Authentication Preventing Signatures

- $\text{Setup} \to (\text{sk}, \text{vk})$
- $\text{Sign}(\text{sk}, \text{msg}) \to \sigma$
- $\text{Verify}(\text{vk}, \text{msg}, \sigma) \to 0/1$
- $\text{Extract}((\text{msg}_1, \sigma_1), \ldots, (\text{msg}_t, \sigma_t)) \to \text{sk}$

  Extraction succeeds if $\phi(\text{msg}_1, \ldots, \text{msg}_t) = 1$

Predicate Authentication Preventing Signatures

- $\mathsf{Setup} \to (\mathsf{sk}, \mathsf{vk})$
- $\mathsf{Sign}(\mathsf{sk}, \mathsf{msg}) \to \sigma$
- $\mathsf{Verify}(\mathsf{vk}, \mathsf{msg}, \sigma) \to 0/1$
- $\mathsf{Extract}((\mathsf{msg}_1, \sigma_1), \ldots, (\mathsf{msg}_t, \sigma_t)) \to \mathsf{sk}$

  Extraction succeeds if $\phi(\mathsf{msg}_1, \ldots, \mathsf{msg}_t) = 1$

  DAPS is a special case for predicate

$$\phi((\mathsf{subj}_1,\mathsf{payload}_1), (\mathsf{subj}_2, \mathsf{payload}_2)) = \begin{cases} 1 & \mathsf{subj}_1 = \mathsf{subj}_2 \land \mathsf{payload}_1 \neq \mathsf{payload}_2 \\ 0 & \text{Otherwise} \end{cases}$$

Open Problems

- **Theoretical**: Can we construct PAPS for more general circuit classes?
- **Practical**: What are some practical holes for implementing DAPS in the real world?

Open Problems

- **Theoretical**: Can we construct PAPS for more general circuit classes?
- **Practical**: What are some practical holes for implementing DAPS in the real world?

Thanks!