A generic view on trace-and-revoke broadcast encryption schemes

Dennis Hofheinz and Christoph Striecks

Karlsruhe Institute of Technology, Germany

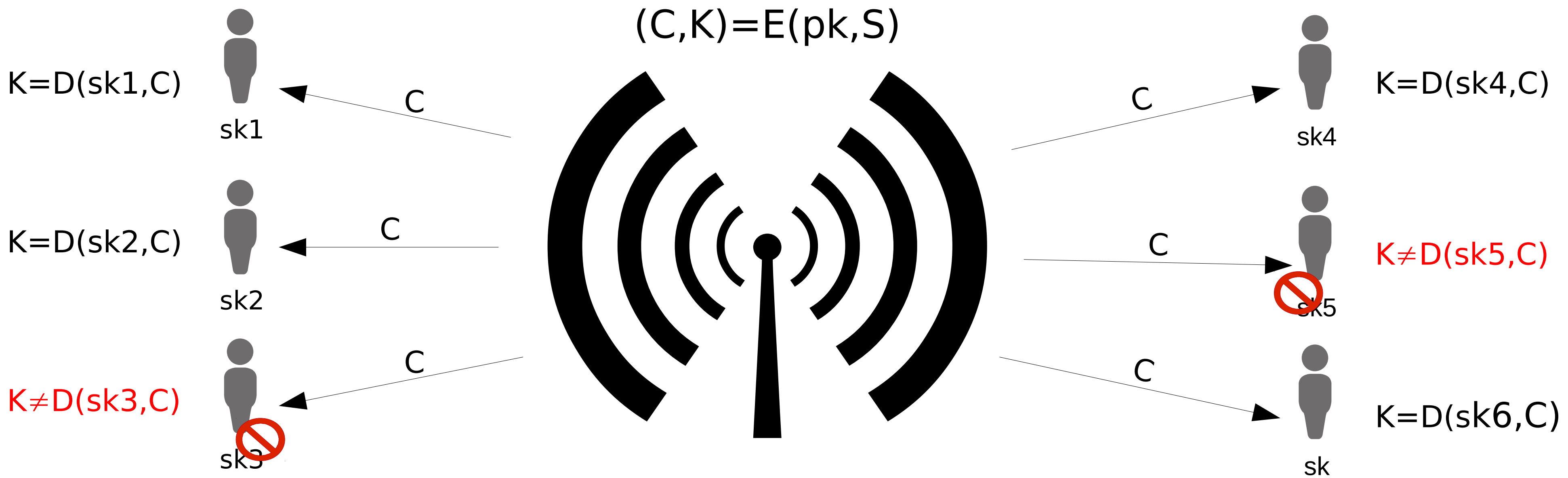
Overview

- New generic view on trace-and-revoke schemes from (generic) Extended DDH (EDDH) assumption [HO12]
- 1st result: EDDH-based threshold PKE/signatures, revocation schemes (extends [Wee11])
- 2nd result: (mild) traceability of EDDH-based revocation schemes
- 1st + 2nd: new (generic view of) EDDH-based trace-and-revoke schemes

Broadcast encryption [FN93]

Goal: est. a shared symm. key betw. sender and privileged set S of users, say, S={1,2,4,6}⊆{1,...,6}

(pk,sk1,...)=Gen(1^k,N=6)



Trivial system:	|C|=O(|S|)	|sk|=O(1)	|pk|=O(N)
[e.g.,BGW05*,D07,SF07,PPSS13,BZ13]:	|C|=O(1)	|sk|=O(1)	|pk|=O(N)
[GW09,PPSS13,BZ13]:	adapt. security		

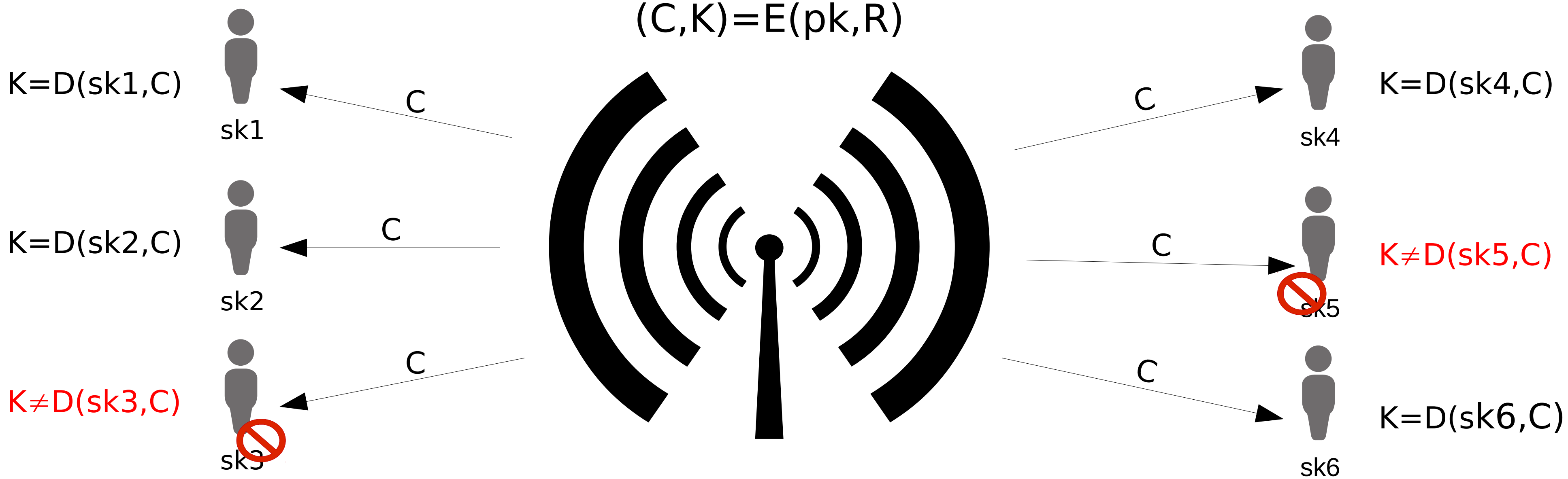
* provide also a system with |C|=O(√N) and |pk|=O(√N)

Our focus: revocation schemes

Consider a set of revoked users,
say, R={3,5}

$(pk,sk1,\ldots)=Gen(1^k,1^t,N=6)$

$(C,K)=E(pk,R)$



[e.g.,NP00,DF03,DPP07,W11]:	$\lvert C\rvert=O(\lvert R\rvert)$	$\lvert sk\rvert=O(1)$	$\lvert pk\rvert=O(\lvert R\rvert)$
[e.g.,NNL01*,HS02*,DF02]:	$\lvert C\rvert=O(\lvert R\rvert)$	$\lvert sk\rvert=O(\log N)$	$\lvert pk\rvert=O(1)$
[LSW10]:	$\lvert C\rvert=O(\lvert R\rvert)$	$\lvert sk\rvert=O(1)$	$\lvert pk\rvert=O(1)$

* only secret-key schemes; parameters improved by [GST04]

Generic revocation schemes and threshold extractable hash proof systems [Wee11]

- Previous revocation schemes use Shamir's secret sharing (i.e., Lagrange interpolation) in the exponent [e.g.,NP00]
- [W11] gives a simple and elegant view of revocation schemes using TEHPSs

- Gen(1^k,1^t,N): $pk = g^{a_0}, g^{a_1}, \ldots, g^{a_t}$

  $\text{sec. polyn. } f(x) = a_0 + a_1 x + \ldots + a_t x^t$

  $sk_j = f(j),\ j \in [N]$

- E(pk,R): $C = \left(R, u, \left(u^{f(i)}\right)_{i \in R}\right), u = g^r, \text{rand. } r, |R| = t$

  $K = G\left(u^{f(0)}\right)$

- D(sk_j,C): $j \notin R: \text{with } u^{sk_j} = u^{f(j)}, \text{all } \left(u^{f(i)}\right)_{i \in R}, \text{interpol. } u^{f(0)}$

  $\text{for Lagr. coeff. } L_j(0) = \prod \frac{-i}{j - i}$

  $K = G\left(u^{f(0)}\right)$

- Depending on G, this yields rev. schemes from factoring, CDH, and DDH

1st result: slightly different view of [W11]

- Based on Extended DDH assumpt. [HO12] (which general. DDH, DCR):

$$\left(g, g^{a}, g^{r}, g^{a \cdot r}\right) \approx \left(g, g^{a}, g^{r}, g^{a \cdot r} \cdot h\right)$$

$$\text{for } G', H \subseteq G, \text{ rand. } g \in G', h \in H, \text{exp. } a, r$$

- But now: order of G' might be unknown (i.e., with DCR); hence, difficult to interpolate in the exponent, i.e.,

$$\text{how to compute Lagr. coeff. } L_j(0) = \prod \frac{-i}{j-i} \text{ in the exponent?}$$

- Solution: "clearing the denominator in the exponent" [S00], i.e.,

$$\text{use } D = \text{lcm}\left\{\prod_{i,j,i \neq j} (j-i)\right\} \text{ s.t. } DL_j(0) \text{ is an integer}$$

- As a result: we derive EDDH-based TEHPSs, i.e., EDDH-based threshold PKE/signatures, revocation schemes

In detail: EDDH-based rev. schemes

- $\mathrm{Gen}(1^k, 1^t, N)$: $pk = g^{a_0}, g^{a_1}, \ldots, g^{a_t}$ with sec. polyn. $f(x) = a_0 + a_1 x + \ldots + a_t x^t$

  $sk_j = f(j),\ j \in [N]$

- $\mathrm{E}(pk, R)$: $C = \left(R, u_1, \left(u_1^{f(i)}\right)_{i \in R}, u_2\right), u_1 = g^r, u_2 = u_1^{f(0)} \cdot h$, rand. r, h

  $K = G(h)$

- $\mathrm{D}(sk_j, C)$: $j \notin R$: with $u_1^{sk_j} = u_1^{f(j)}$, all $\left(u_1^{f(i)}\right)_{i \in R}$, interpol. $u_1^{f(0)}$

  for Lagr. coeff. $L_j(0) = \prod \frac{-i}{j-i}$

  and $D = \mathrm{lcm}\left\{\prod_{i, j, i \neq j} (j - i)\right\}$ such that

  $$\left(\left(\prod u_1^{D L_j(0) f(j)}\right)^{-1} \cdot u_2^D\right)^{D^{-1} \bmod n} = h$$

  $K = G(h)$

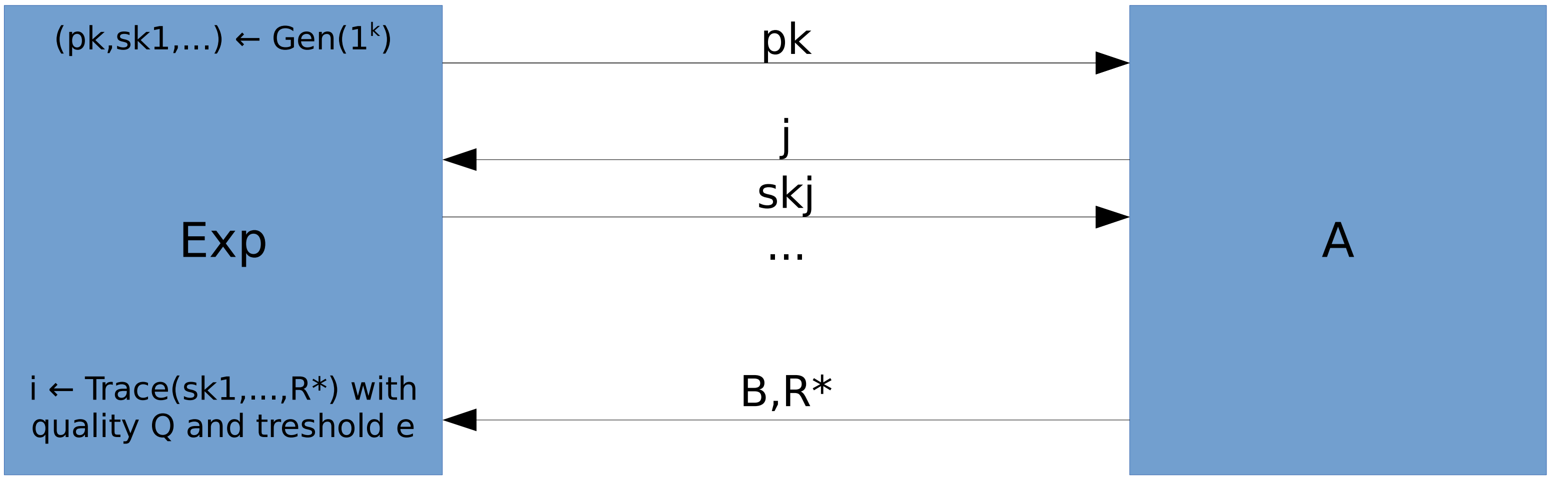
- Special case: yields DCR-based rev. schemes (uses a potential stronger assumpt. than Wee's fact.-based inst. but, via our 2nd result, yields new DCR-based trace-and-revoke schemes, which is not known from factoring)

Traceability [CFN94]

- Ability to trace a pirate dec. box back to its (corrupt.) creator(s)

[e.g.,NP98,BF99,GSY99,NP00,NNL01,TT01,KY01b,KY02,HS02,DF02,DF03, KHL03,DFKY05,BSW06,BW06,JL07,FA08,KP09,AKPS12,...]

- Here, consider traceability model in the rev. setting:



A wins iff Q>e and A never queried a secret key for i;
rev. system is traceable iff Pr[A wins]=negl.

- Results in trace-and-revoke schemes (non-trivial to achieve [BW06])

Traceability in our concrete setting

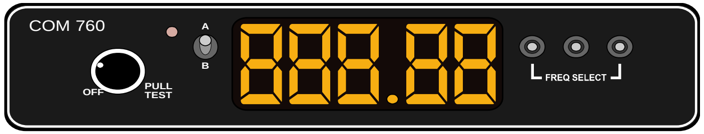
Ciphertext C

D(sk_j,C)=K'?

C

K'

(Stateless) black-box decoder B



- Observation: decryption of ciphertext C, where (C,K)=E(pk,R), does not depend on a user secret key (i.e., D(sk_j,C)=K, for all j∉R)
- Thus: we have to generate random ciphertexts
- But: these ciphertexts must be indistinguishable to real ctexts for B
- Further: B might only decrypt correctly down to some threshold e
- Previous work: [TT01] assumes e=1 and no adv. chosen R while [DFKY05] considered diff. scheme

2nd result: our tracing strategy of rev. instances

- Consider random ciphertexts in the EDDH-based rev. setting:

$$C_{rnd} = \left(R, u_{1,} \left(u_1^{f(i)} h^{z_i}\right)_i, u_1^{f(0)} h^{z_0}\right), \text{ for uniform } h \in H, z_i, z_0$$

- Under EDDH, C_{rnd} is indistinguishable from real ciphertexts (but only for one sk in B!)

- Thus, adapt to allow more sks in B:

$$C_{rnd}^{I} = \left(R, u_{1,} \left(u_1^{f(i)} h^{f'(i)}\right)_i, u_1^{f(0)} h^{f'(0)}\right), \text{ with } f'(i) = 0 \text{ for } i \in I$$

- C^{I}_{rnd} is indist. to a real ciphertext (even when knowing sks for set I)

- Task: find "suspect set" I; unfort., only eff. for polyn. values of $\binom{N}{T}$ with number of traitors T≤(t+1)/2

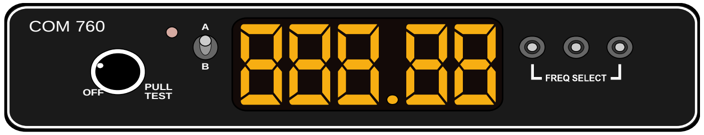
More on our tracing strategy

- If I is found, use standard techniques [e.g.,BF99,NNL01,TT01,KY02, DFKY05,BSW06]:

Rand. ciphertext C^{I}_{rnd} $\xrightarrow{C^{I}_{rnd}}$

$D(sk_j, C^{I}_{rnd}) = K'?$ $\xleftarrow{K'}$

(Stateless) black-box decoder B



Assume B has only user keys for user set ⊆ I

- 1st run: B will decrypt correctly with probability e (i.e., B cannot dist. random from real ciphertexts)

- 2nd run: remove one I-element j and try again with set I'=I\{j} (if B has no sk_j, B does not notice)

- i-th run: if decryption quality drops, we must have removed a traitor

Putting the pieces together

- 1st result: EDDH-based TEHPSs (extends [W11]), i.e., threshold PKE/signatures, revocation schemes from the EDDH assumption
- 2nd result: (mild) traceability of the EDDH-based revocation instances
- 1st + 2nd: new (generic view on) EDDH-based trace-and-revoke schemes which explains (known) DDH-based and (new) DCR-based constructions
- Open problem: not known if factoring-based revocation instances of [W11] are traceable

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Broadcast Steganography
or
How to Broadcast a Secret *Covertly*

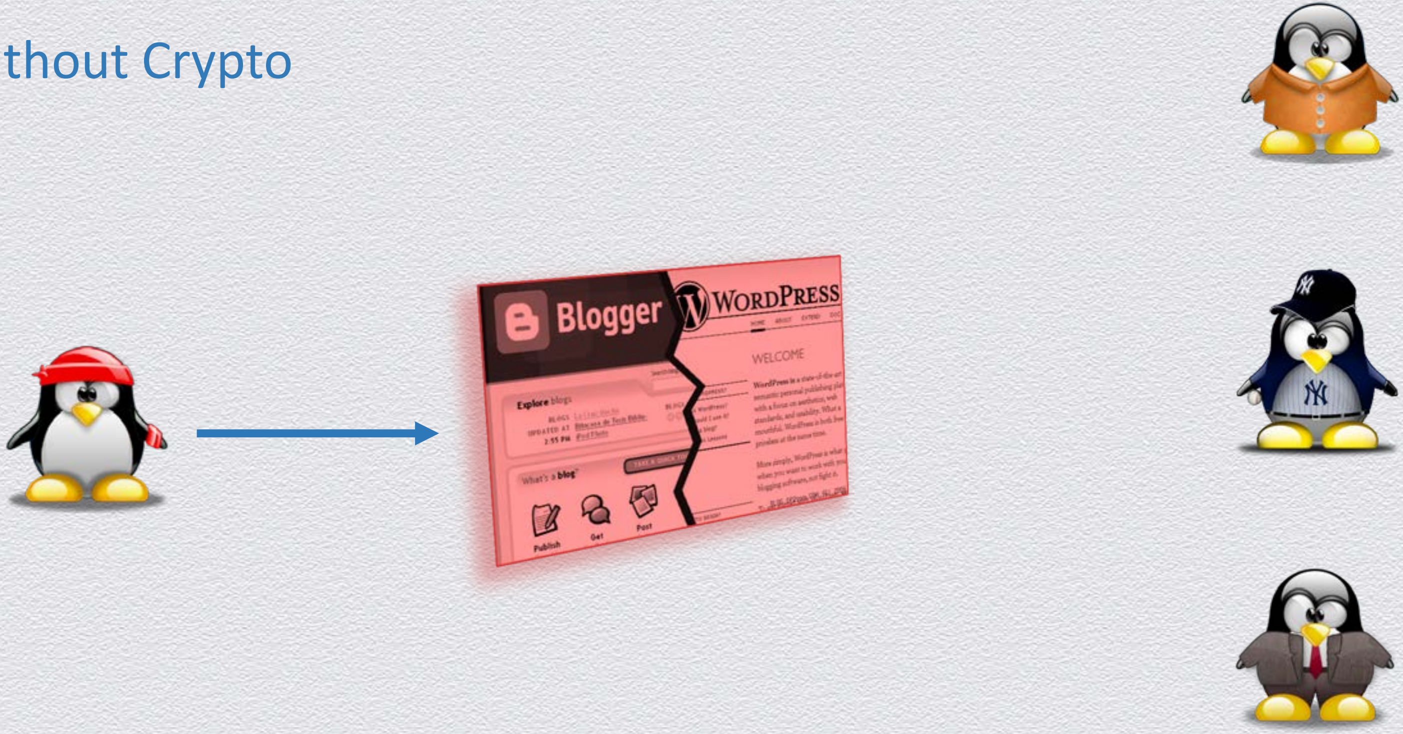
SESSION ID: CRYP-T08

Nelly Fazio
The City College of CUNY
fazio@cs.ccny.cuny.edu

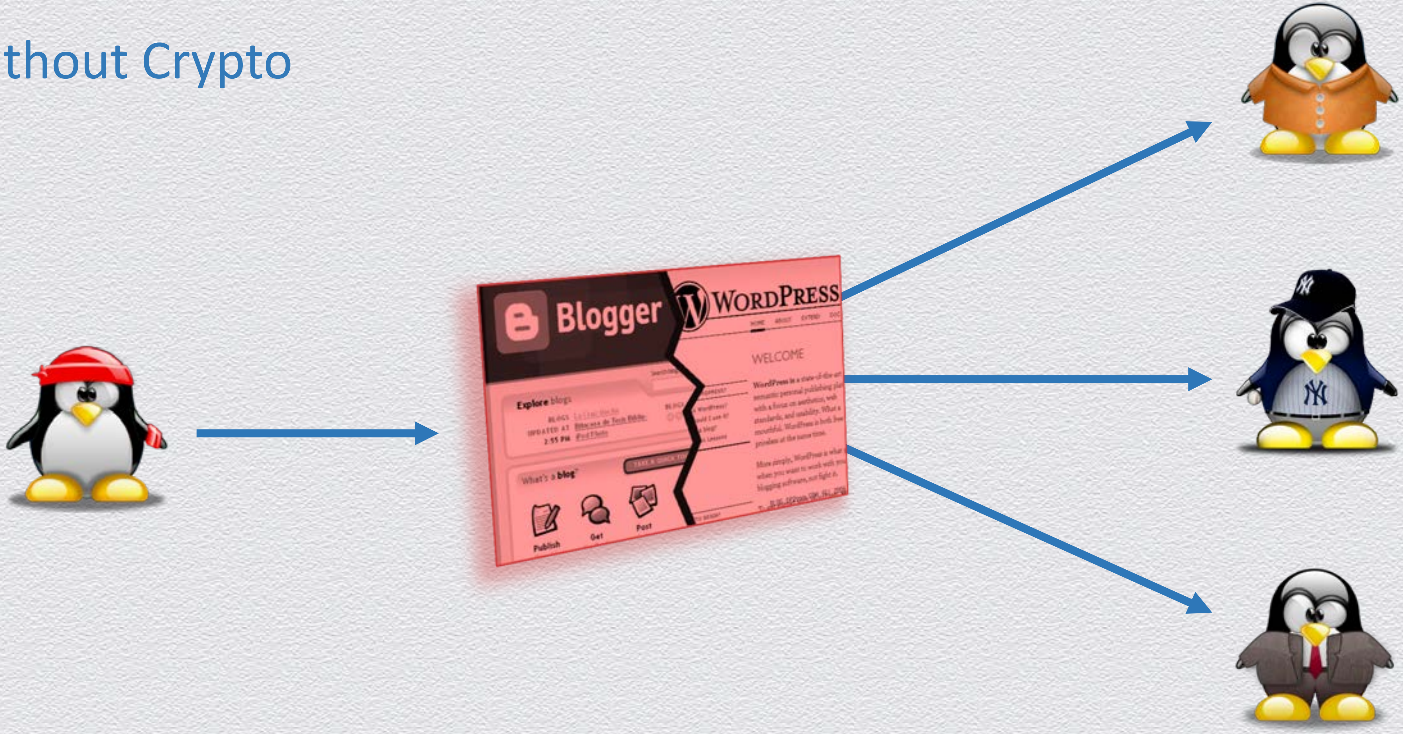
Antonio R. Nicolosi
Stevens Institute of Technology
nicolosi@cs.stevens.edu

Irippuge Milinda Perera
The Graduate Center of CUNY
iperera@gc.cuny.edu

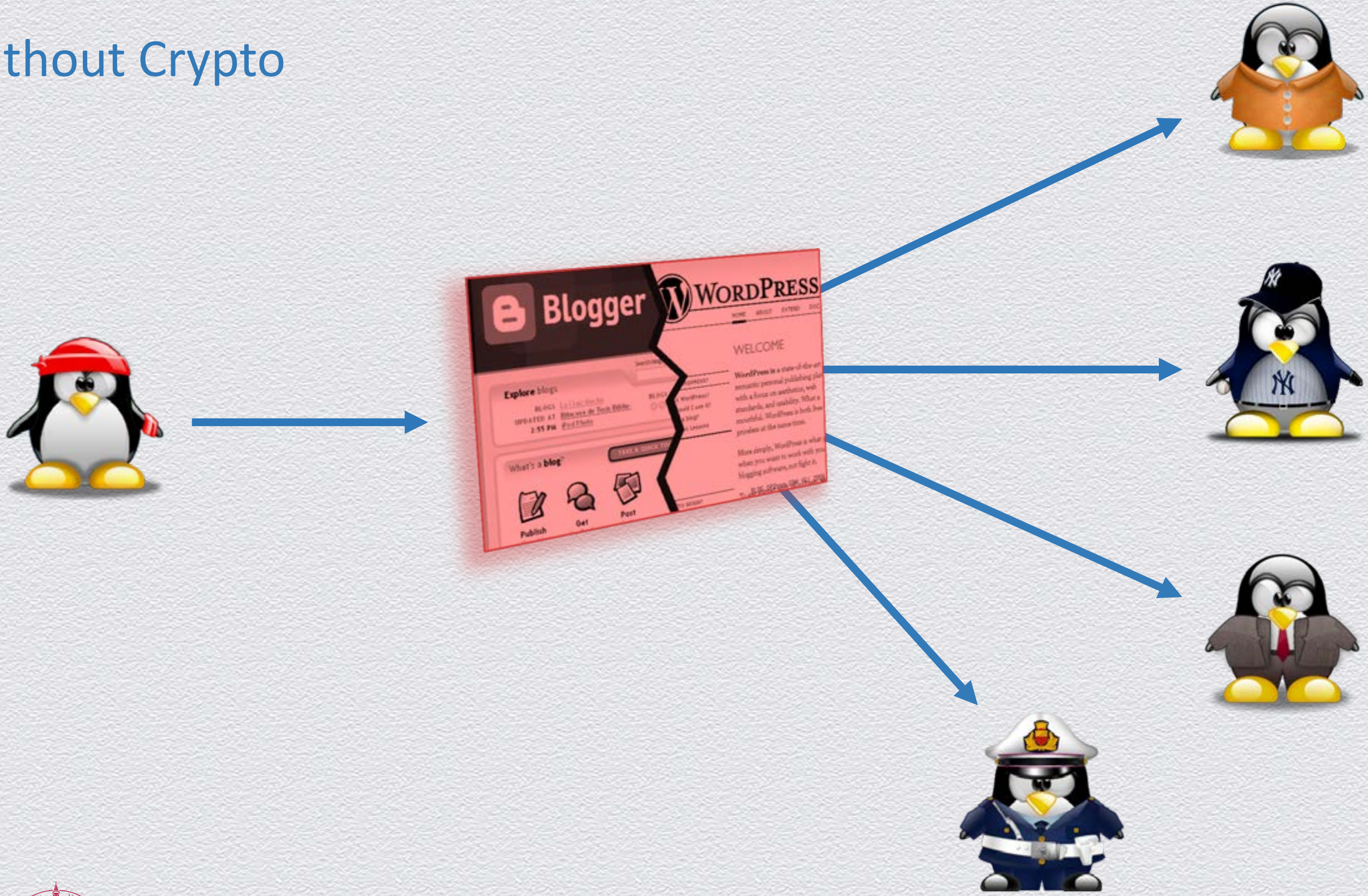
Without Crypto



Without Crypto



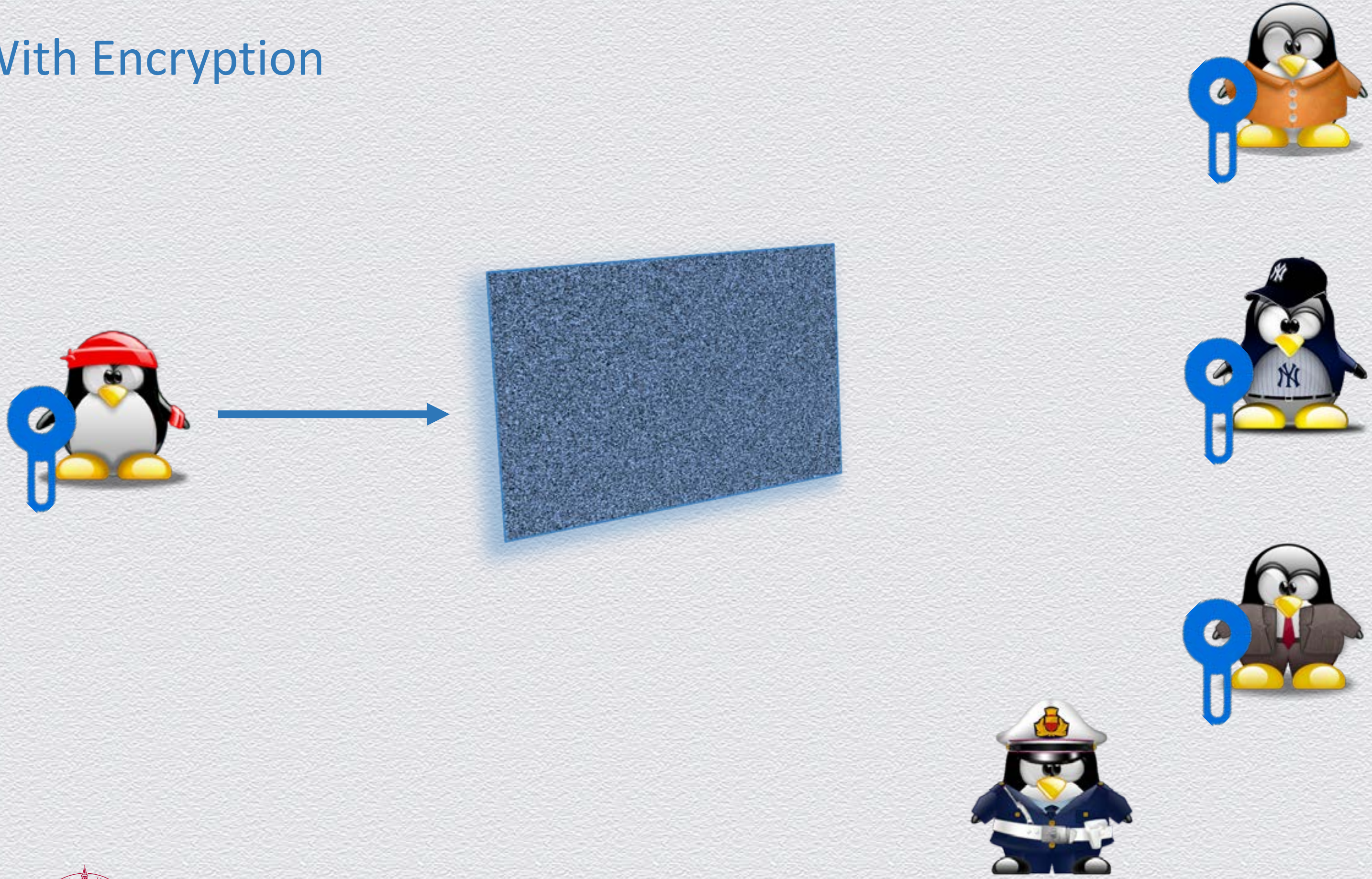
Without Crypto



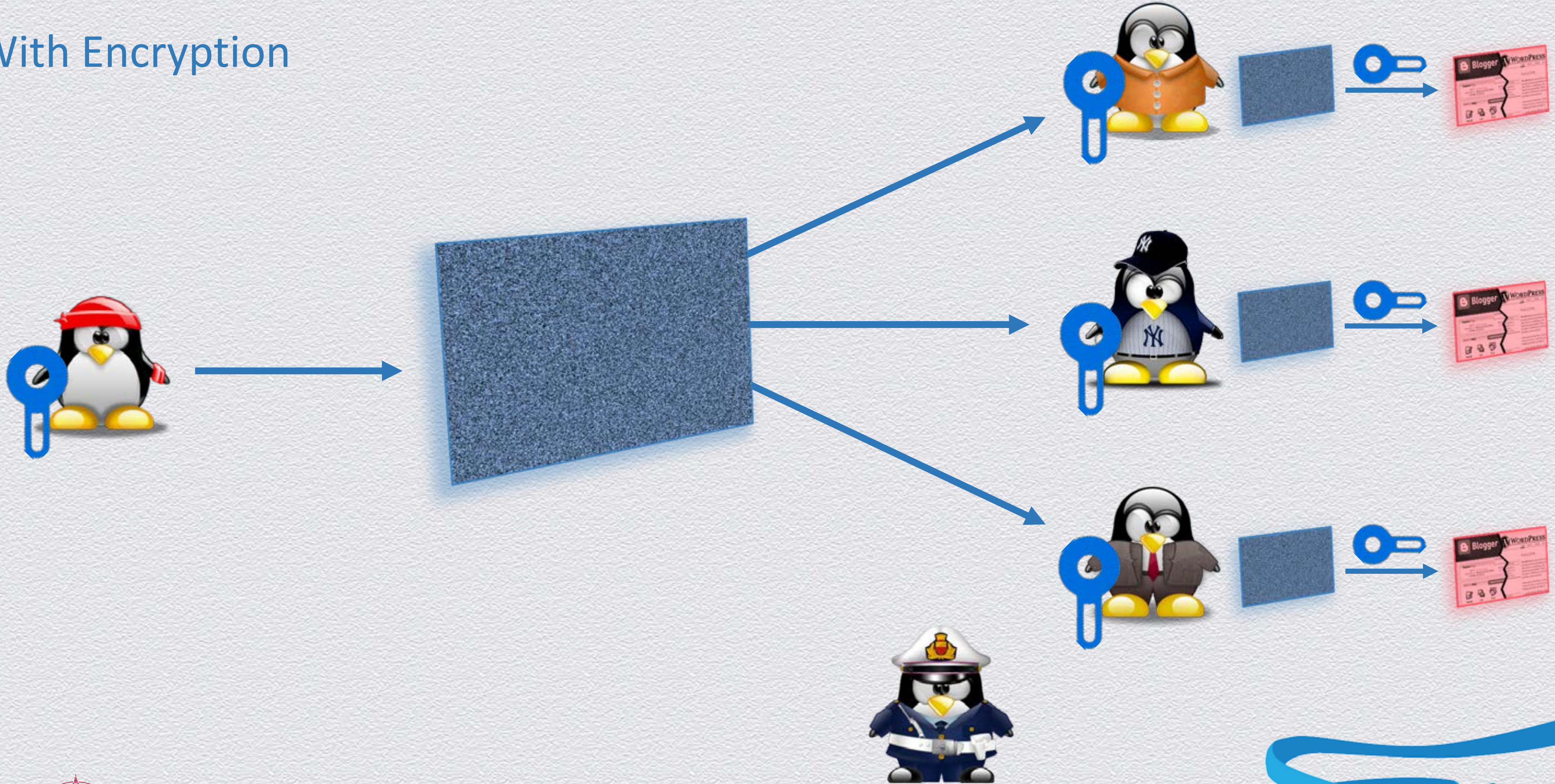
Without Crypto

With Encryption

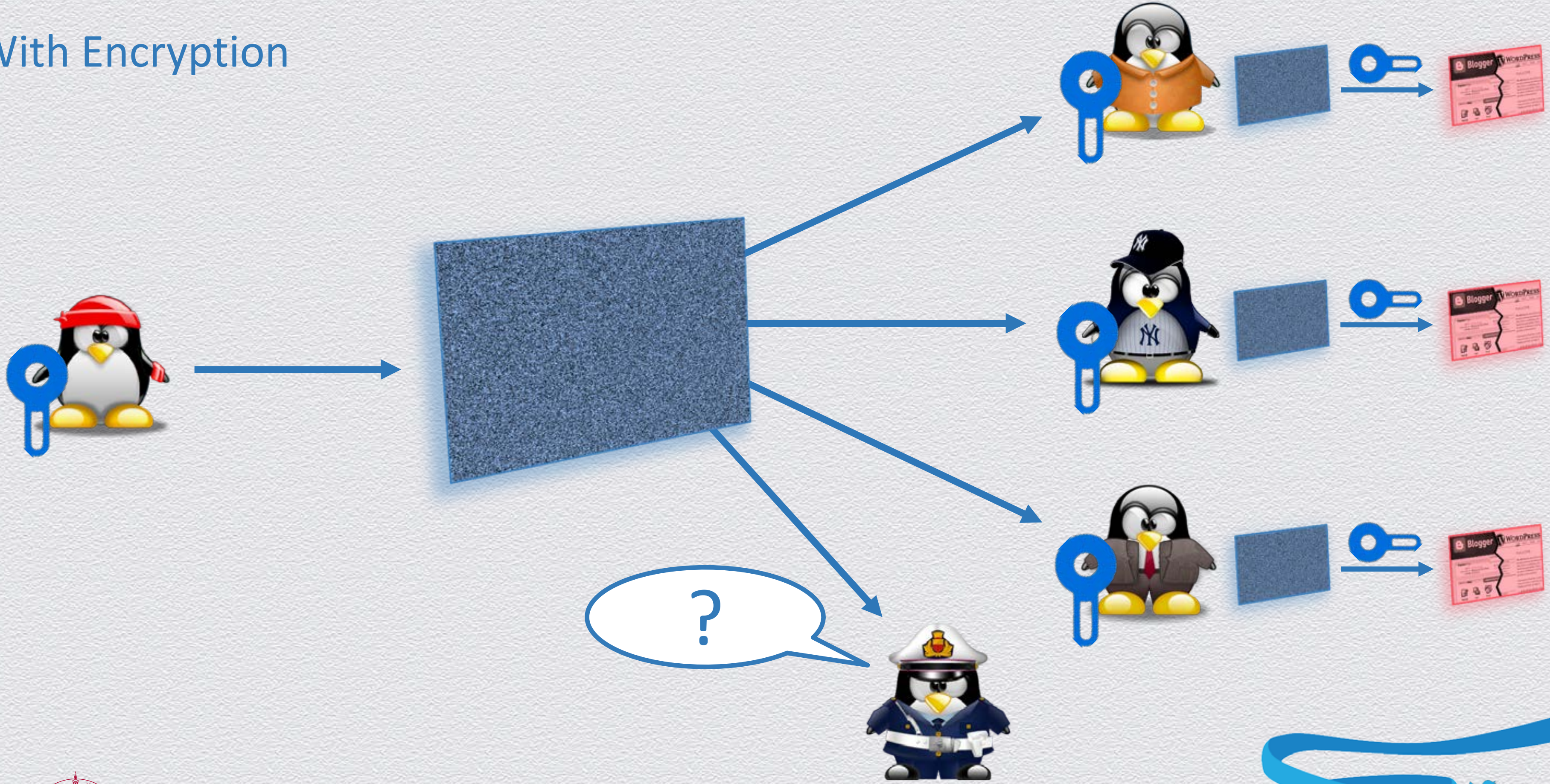
With Encryption



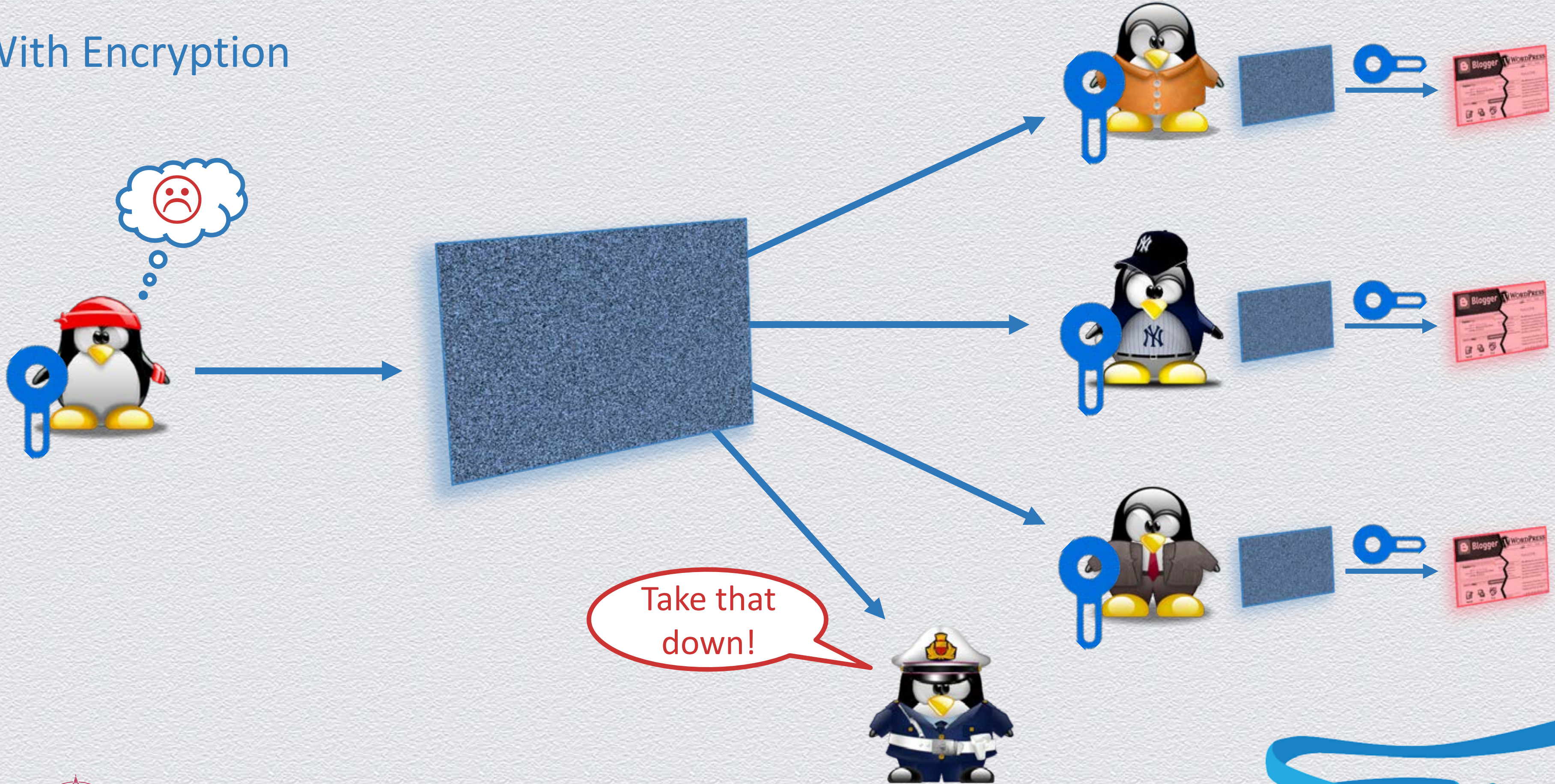
With Encryption



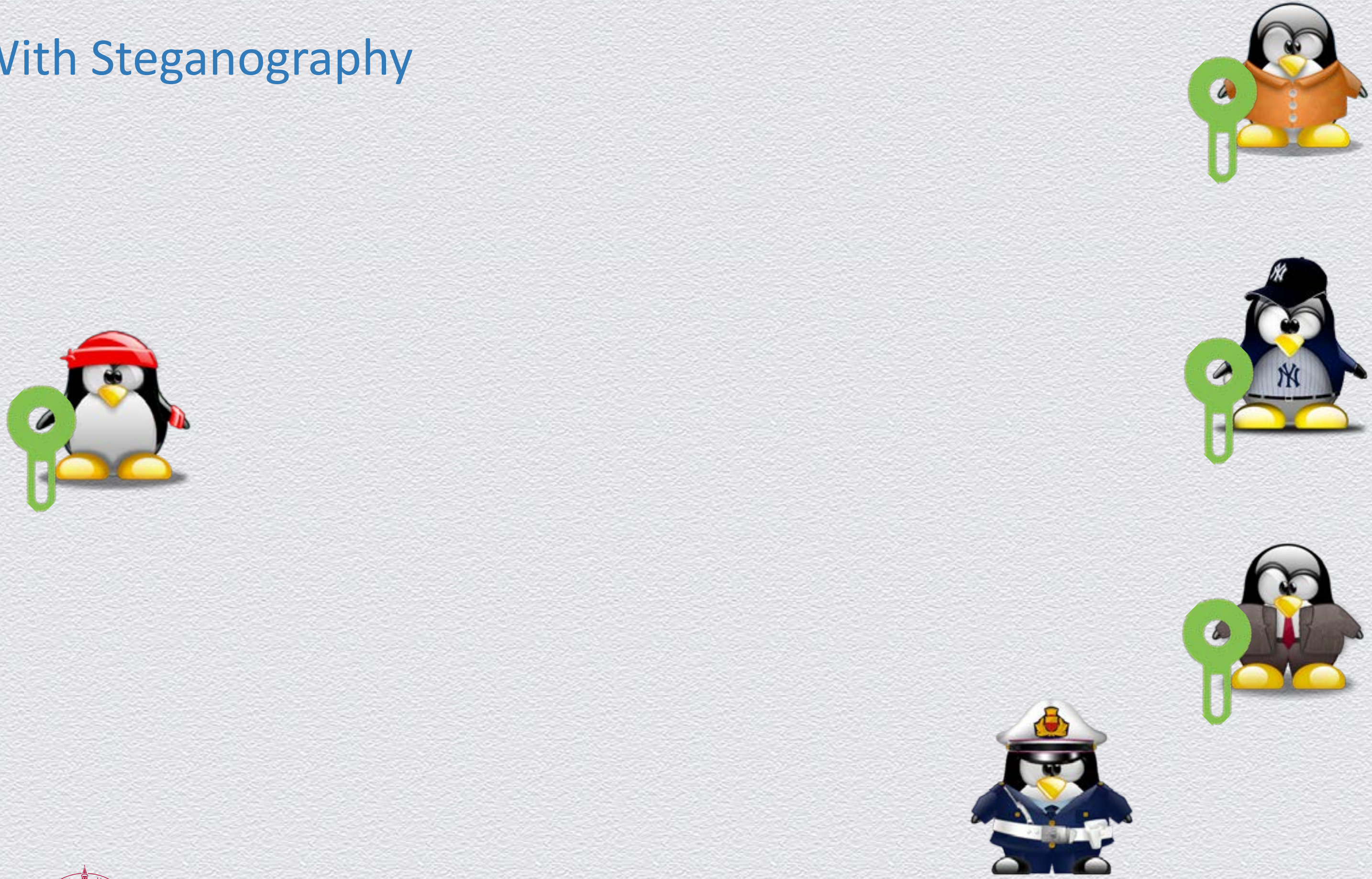
With Encryption



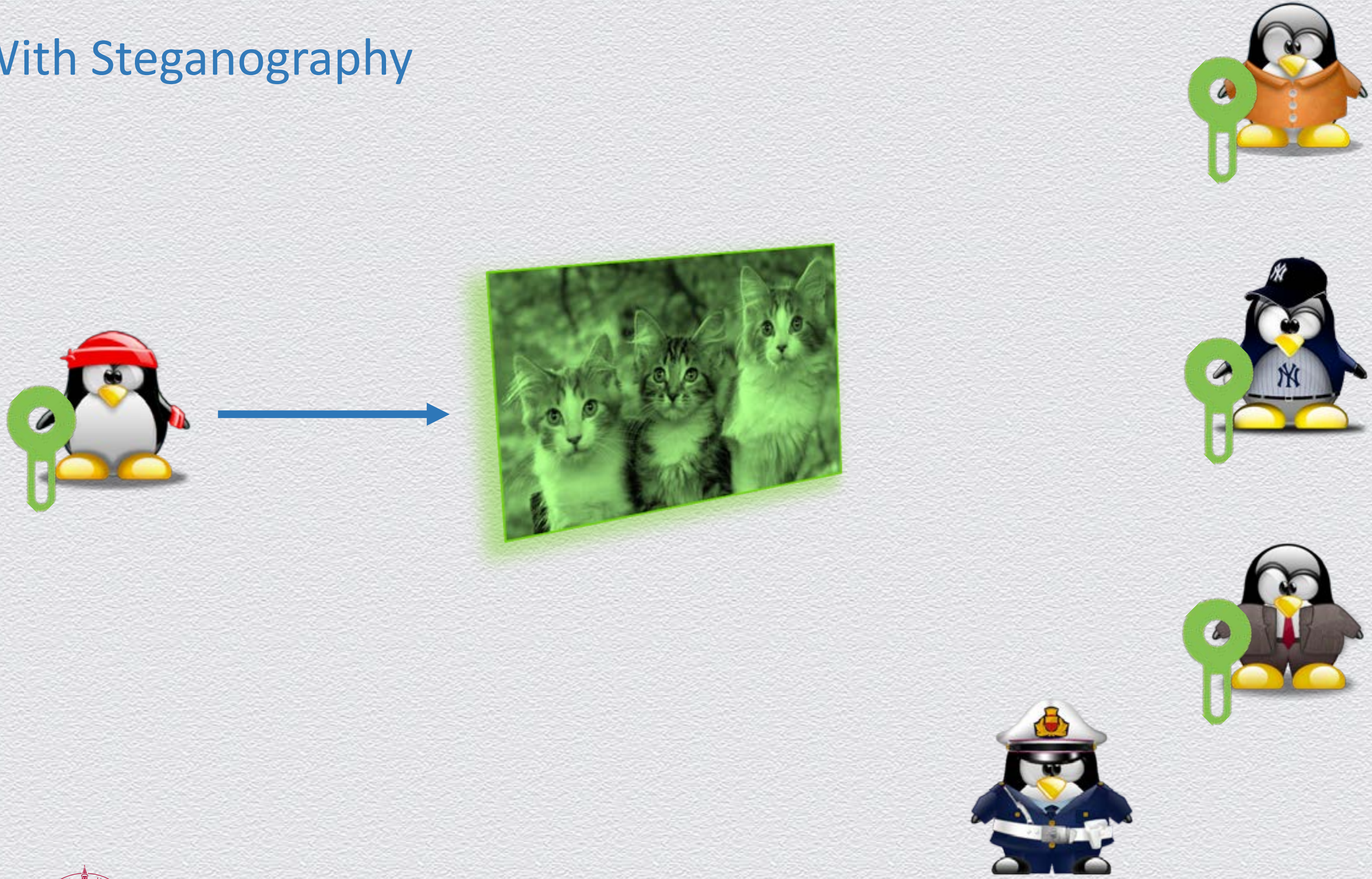
With Encryption



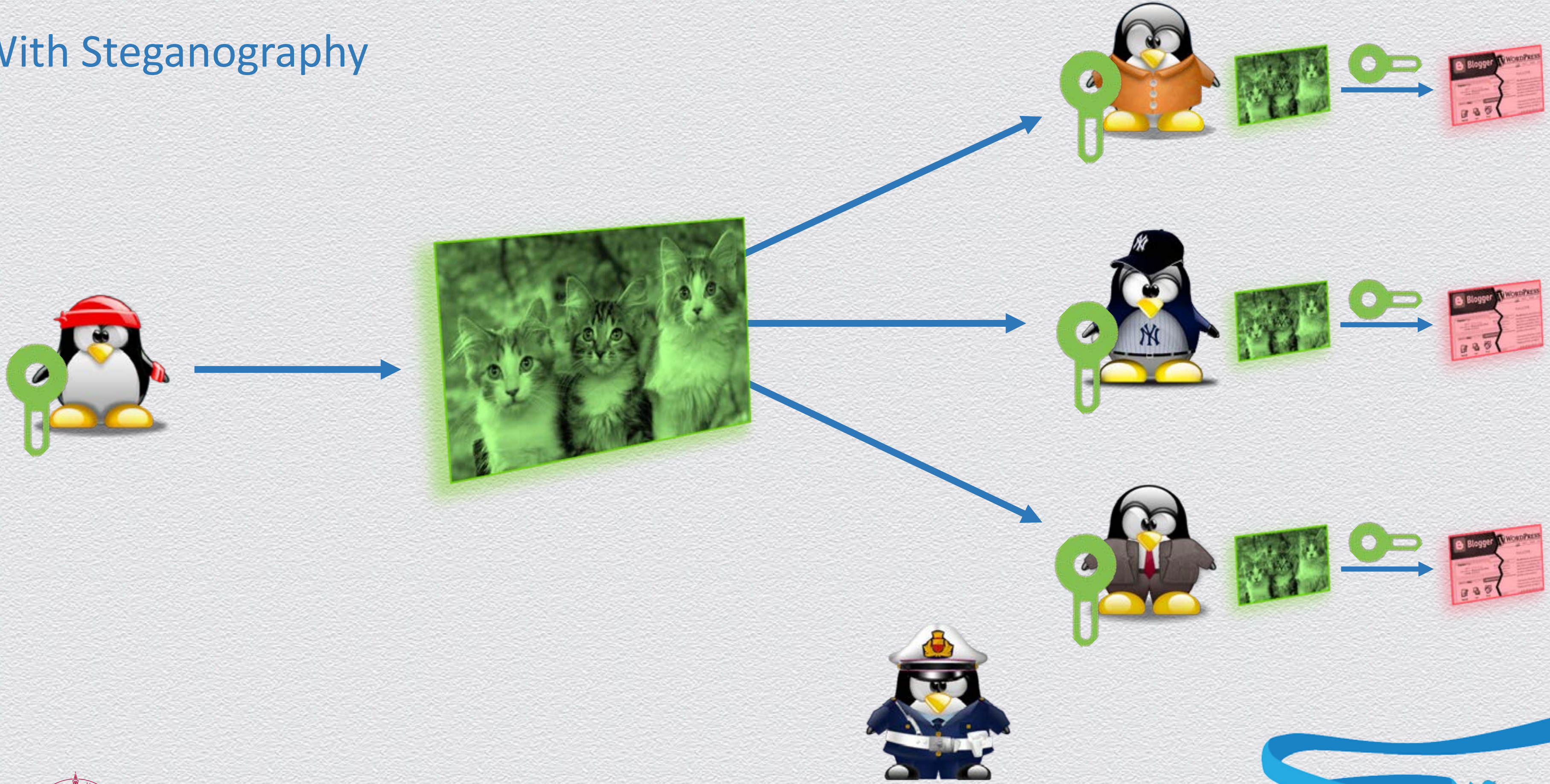
With Steganography



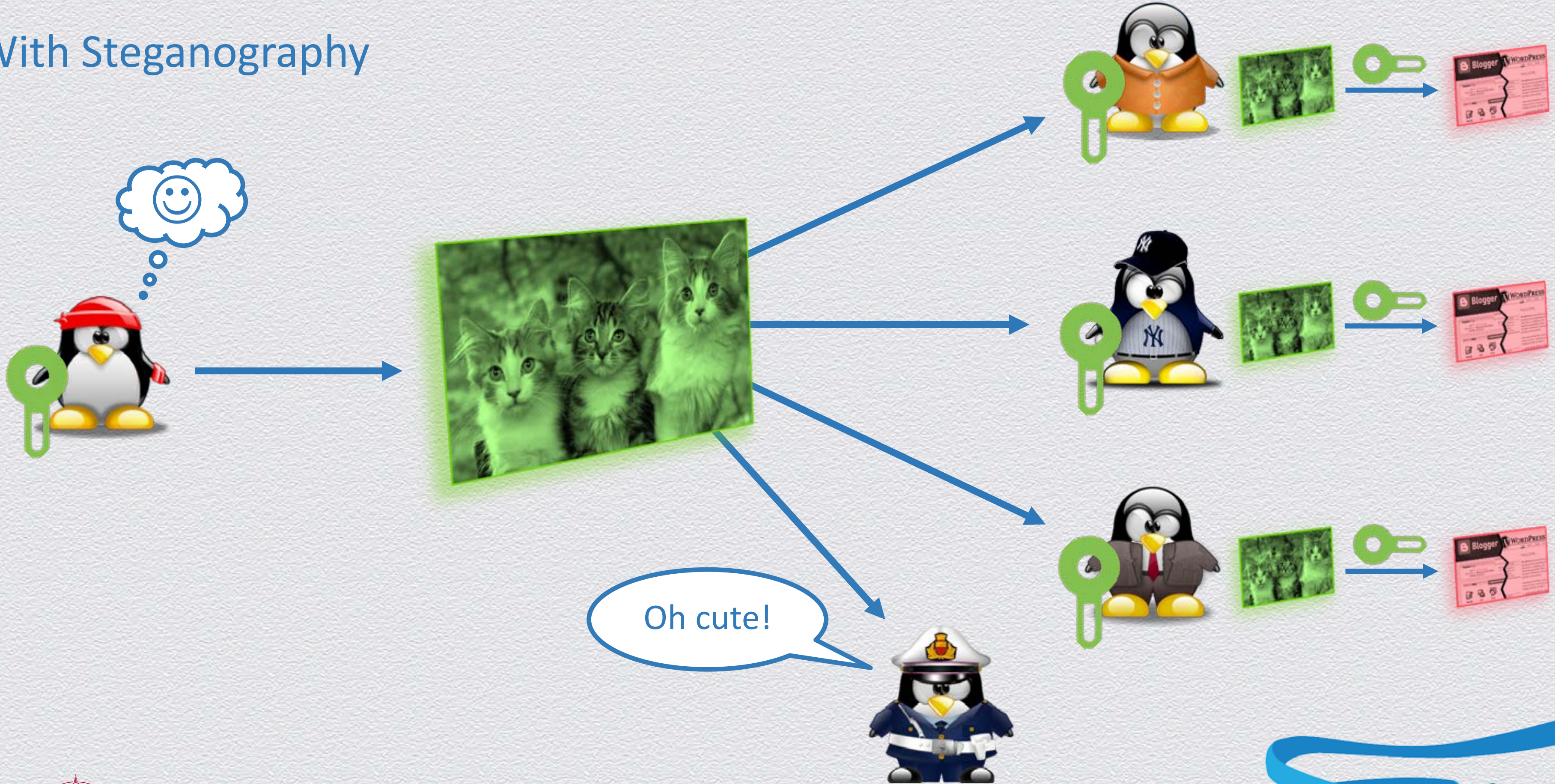
With Steganography



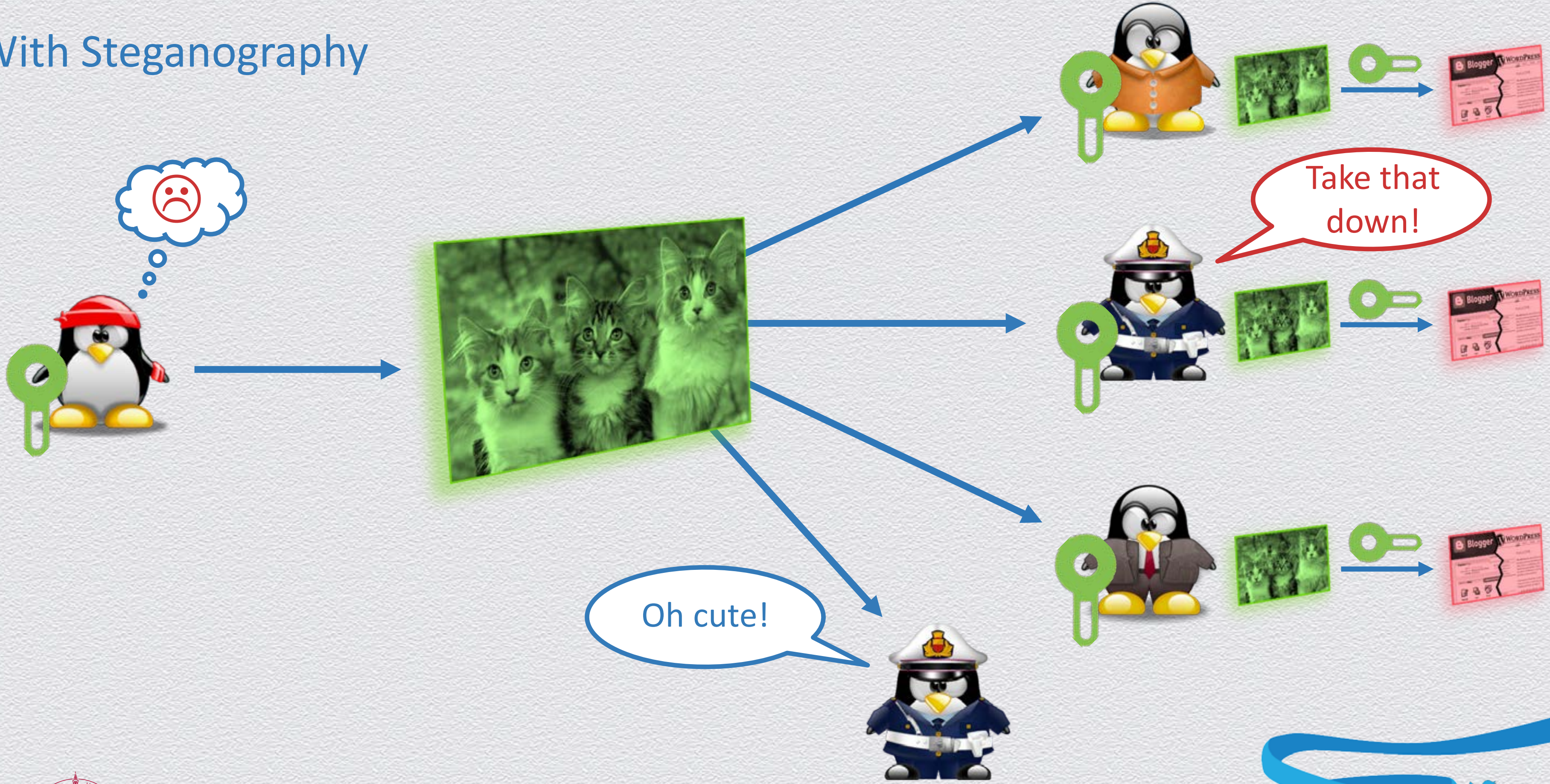
With Steganography



With Steganography

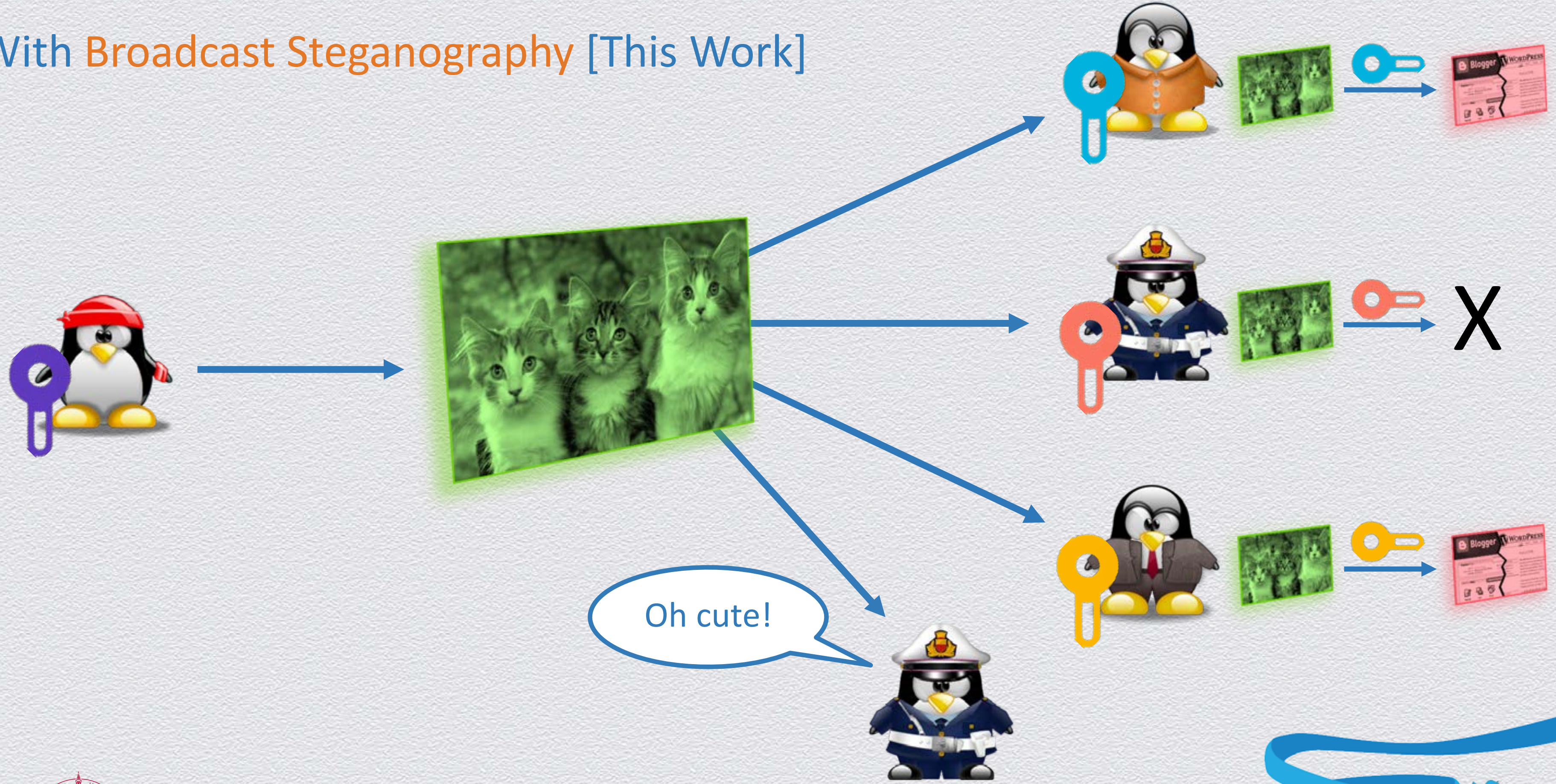


With Steganography

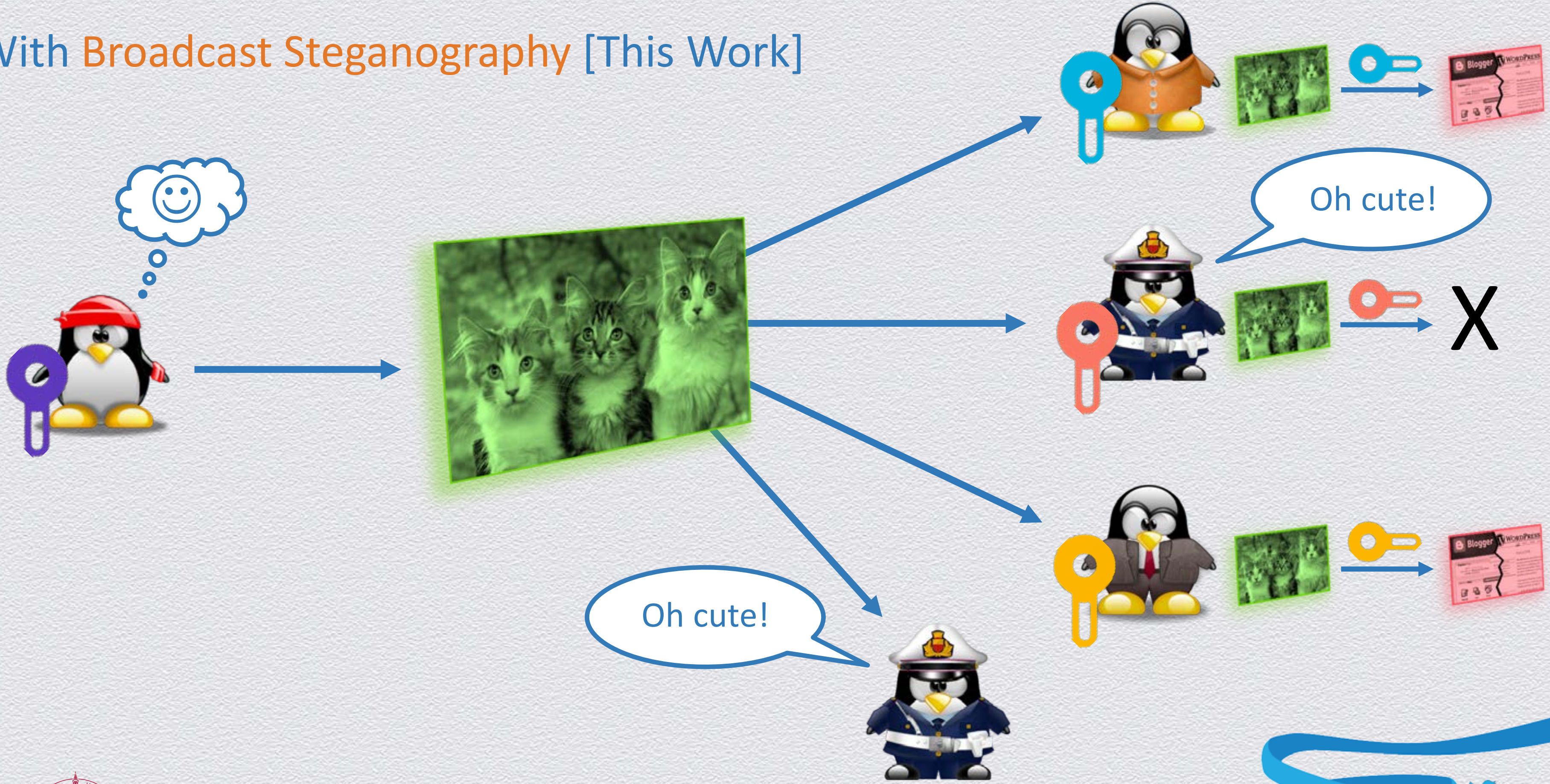


With Broadcast Steganography [This Work]

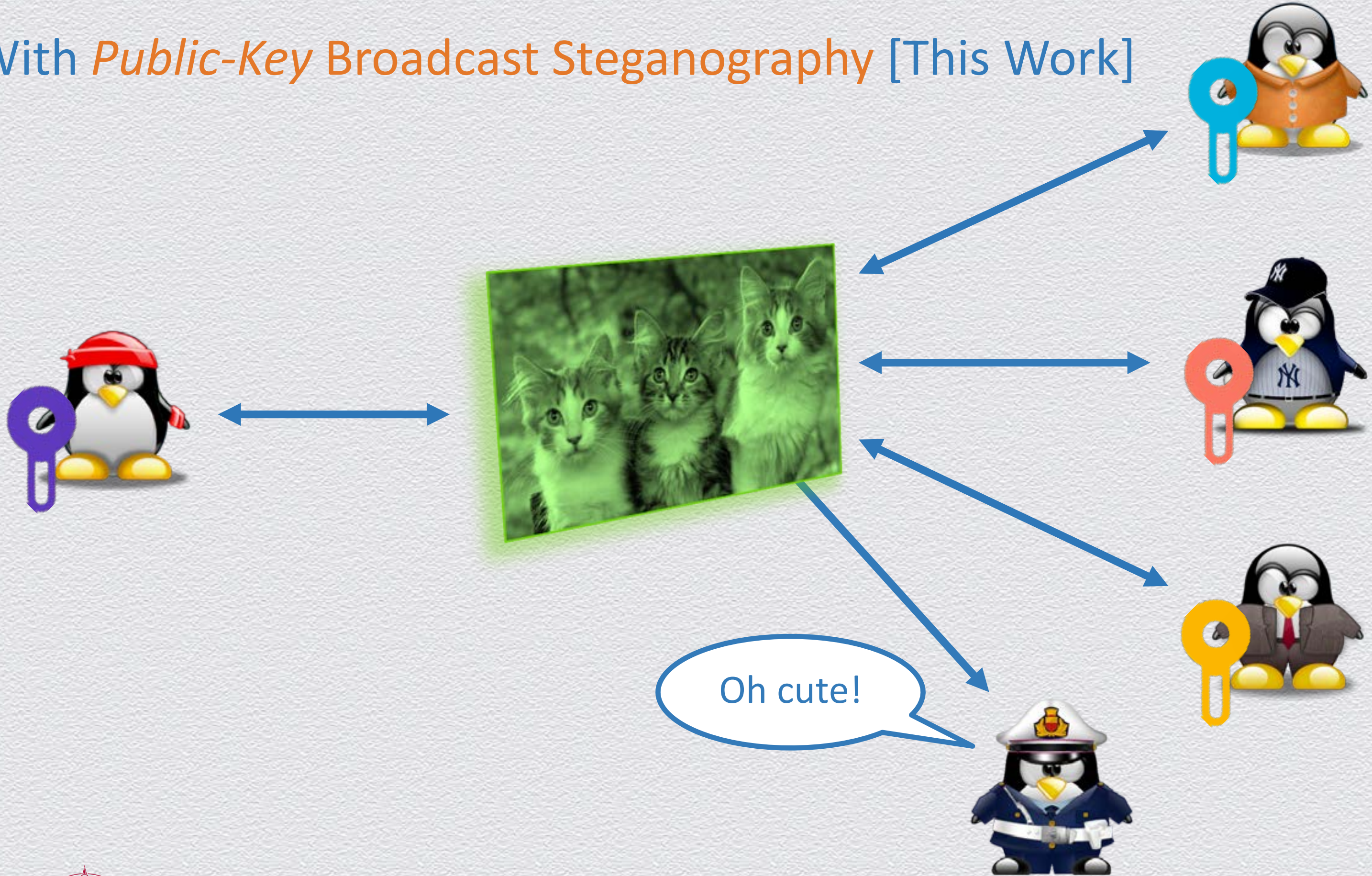
With Broadcast Steganography [This Work]



With Broadcast Steganography [This Work]



With *Public-Key* Broadcast Steganography [This Work]



- Broadcast Steganography (BS)
- Constructions
- Summary

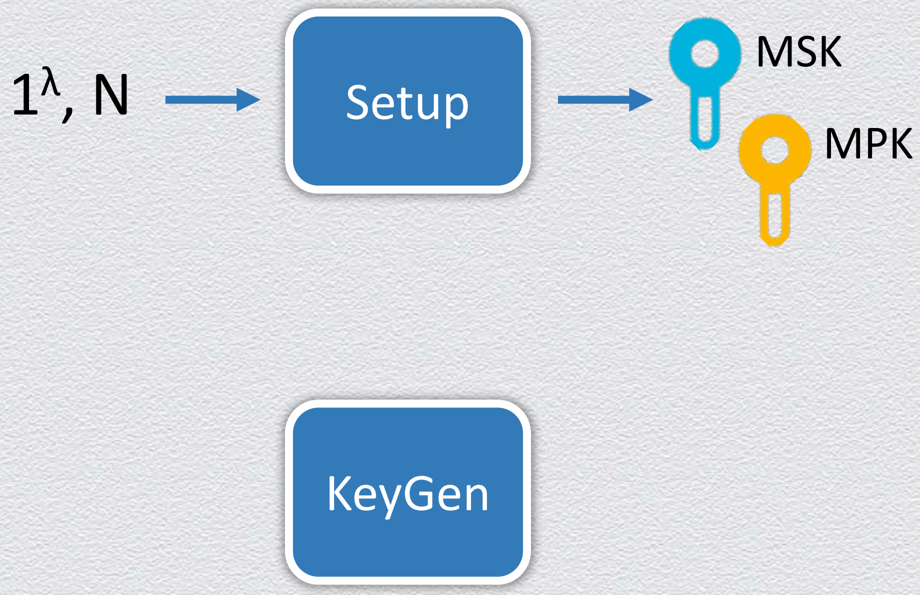
- Broadcast Steganography (BS)
- Constructions
- Summary

The Setting

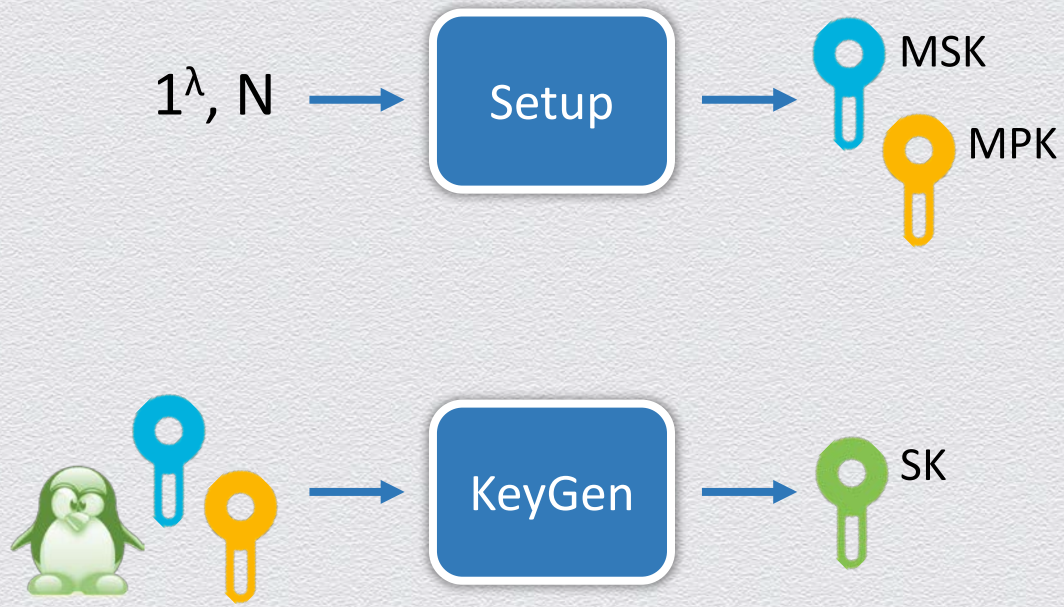
Setup

The Setting

The Setting



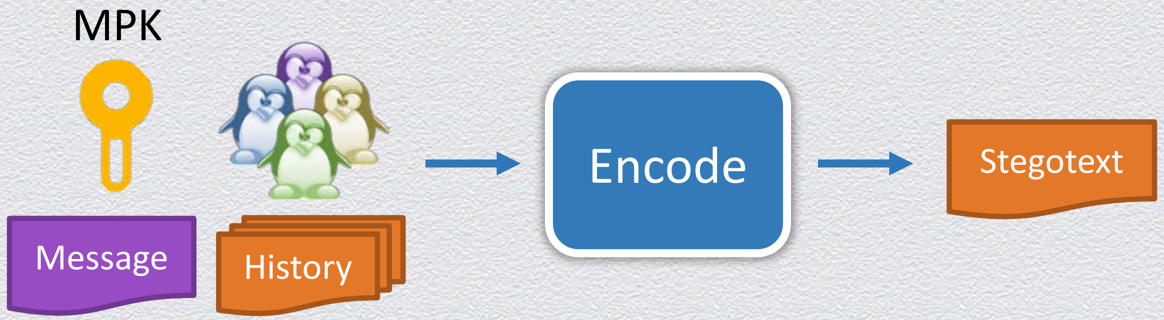
The Setting



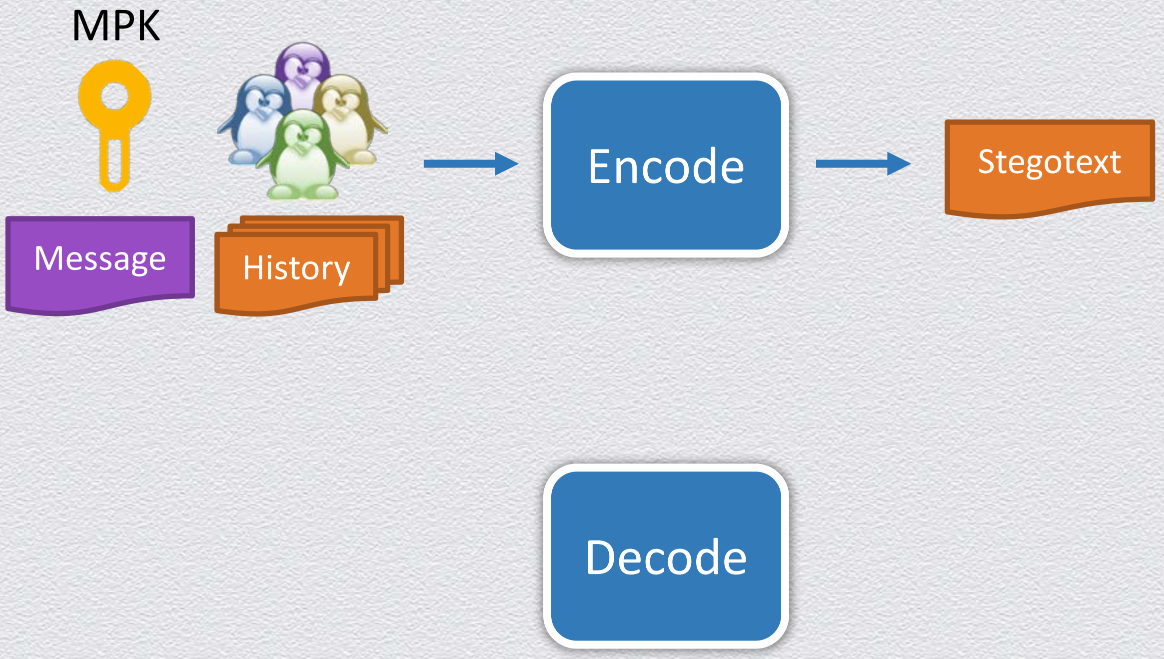
The Setting

Encode

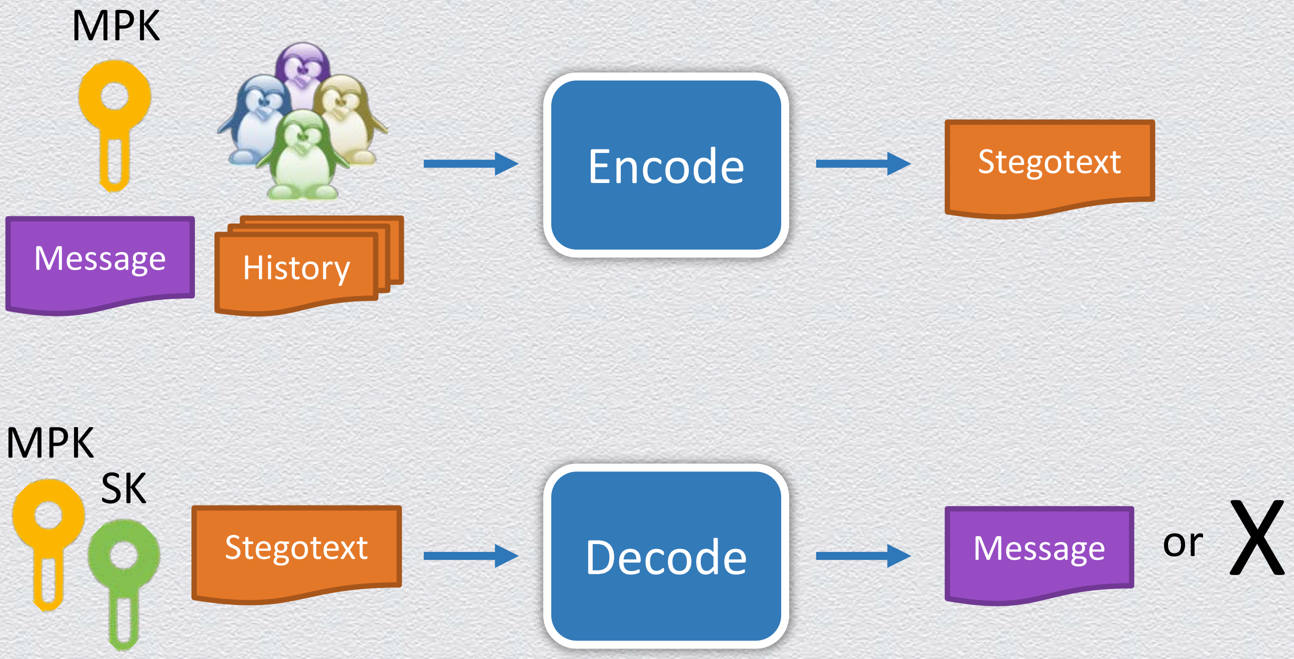
The Setting



The Setting



The Setting


MPK
Message
History
Encode
Stegotext
MPK
SK
Stegotext
Decode
Message
or X

The Security Model

1. Chosen-Covertext Attack (BS-IND-CCA)
   - Analogous to BE-IND-CCA model
   - Adversary is allowed to corrupt users
   - Adversary is also given access to a decoding oracle
2. Publicly-Detectable Replayable Chosen Covertext Attack (BS-IND-PDR-CCA)
   - Similar to BS-IND-CCA, but with stricter restrictions on allowable decoding queries
3. Chosen-Hiddentext Attack (BS-IND-CHA)
   - Analogous to BE-IND-CPA model
   - Adversary is only allowed to corrupt users
   - No decoding queries

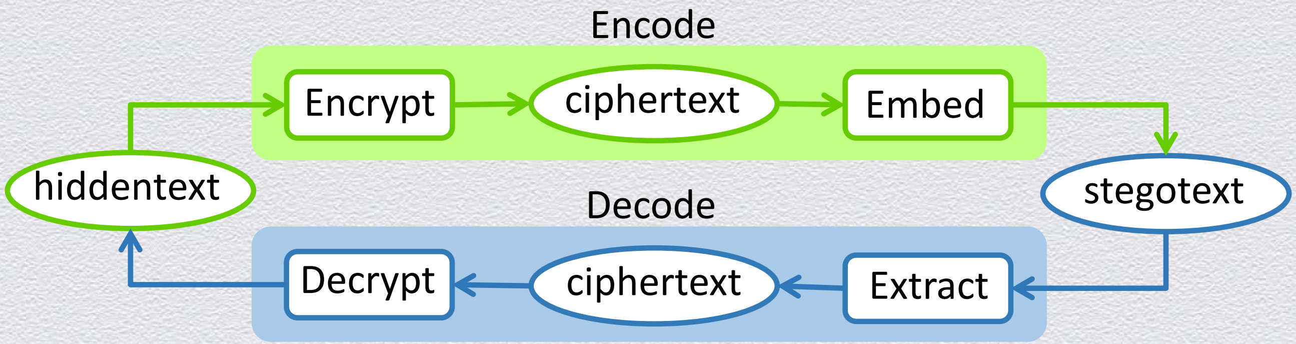
RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

- Broadcast Steganography (BS)
- Constructions
- Summary

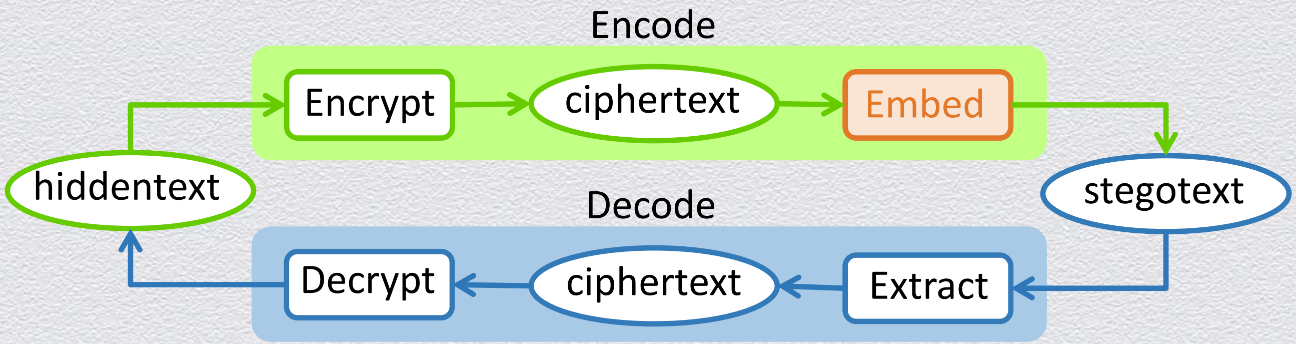
Realizing Broadcast Steganography

- Encrypt-then-Embed Paradigm [HLvA02, BaCa05]



Realizing Broadcast Steganography

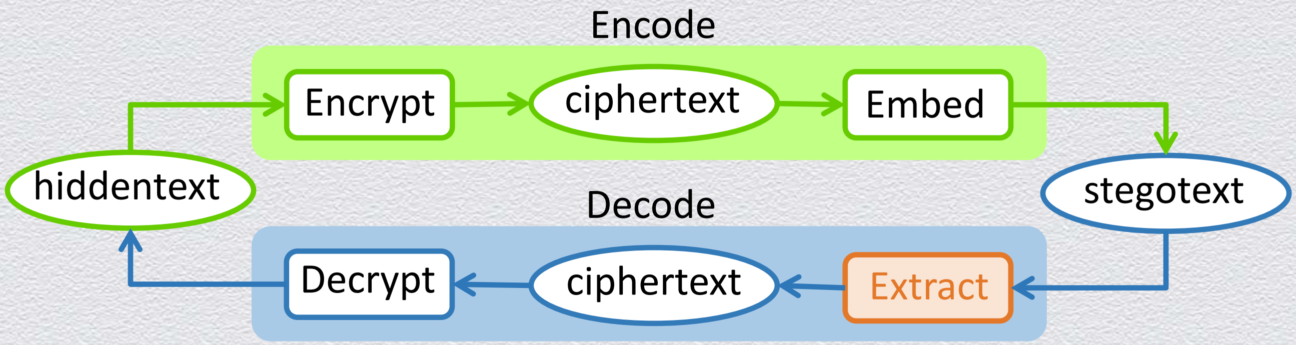
- Encrypt-then-Embed Paradigm [HLvA02, BaCa05]



- Embed (rejection-sampling)
  1. Let H be a strongly universal hash function
  2. Break the ciphertext c into bits $c_1, c_2, \ldots, c_l$
  3. To embed c_i, sample s_i from the channel until $H(s_i) = c_i$
  4. Output $s = s_1 || s_2 || \cdots || s_l$

Realizing Broadcast Steganography

- Encrypt-then-Embed Paradigm [HLvA02, BaCa05]



- Extract
  1. Break the stegotext s into documents $s_1, s_2, \ldots, s_l$
  2. Set $c_i = \mathrm{H}(s_i)$
  3. Output $c = c_1 || c_2 || \cdots || c_l$

Broadcast Encryption + Encrypt-then-Embed = Broadcast Steganography?

- Encrypt-then-Embed requires pseudorandom ciphertexts …
- … but, Broadcast ciphertexts have structure

header	body

broadcast ciphertext format

- Neither header nor body is pseudorandom

Outsider-Anonymous Broadcast Encryption [FaPe12]

- Motivation: Anonymous Broadcast Encryption with short ciphertexts
  - A fully anonymous ciphertext length is subject to a linear lower bound [KiSa12]
  - In some applications, content may give recipient set away
    - ⇒ Suffices to protect anonymity of receivers from outsiders

- Outsider-Anonymity in Broadcast Encryption
  - Trades some degree of anonymity for better efficiency
  - Allows constructions with sub-linear ciphertext length

oABE Encryption in [FaPe12]

- Encrypt(S, m)
  1. Group users in S into S’, a set of disjoint subsets
     - |S’| is sub-linear in |S|
  2. Generate a ciphertext c_i for each s_i in S’ (using anonymous IBE)
  3. Attach a tag t_i to each c_i (for efficient decryption at the receivers)
  4. Bundle all (t_i, c_i) components using one-time signature

oABE Encryption in [FaPe12]

- Encrypt(S, m)
  1. Group users in S into S', a set of disjoint subsets
     - |S'| is sub-linear in |S|
  2. Generate a ciphertext c_i for each s_i in S' (using anonymous IBE)
  3. Attach a tag t_i to each c_i (for efficient decryption at the receivers)
  4. Bundle all (t_i, c_i) components using one-time signature

oABE Encryption in [FaPe12]

- Encrypt(S, m)
  1. Group users in S into S', a set of disjoint subsets
     - |S'| is sub-linear in |S|
  2. Generate a ciphertext c_i for each s_i in S' (using anonymous IBE)
  3. Attach a tag t_i to each c_i (for efficient decryption at the receivers)
  4. Bundle all (t_i, c_i) components using one-time signature

c_1	…	c_l

oABE Encryption in [FaPe12]

- Encrypt(S, m)
  1. Group users in S into S', a set of disjoint subsets
     - |S'| is sub-linear in |S|
  2. Generate a ciphertext c_i for each s_i in S' (using anonymous IBE)
  3. Attach a tag t_i to each c_i (for efficient decryption at the receivers)
  4. Bundle all (t_i, c_i) components using one-time signature

$\boxed{t_0}\ \boxed{t_1 \mid c_1}\ \cdots\ \boxed{t_l \mid c_l}$

oABE Encryption in [FaPe12]

- Encrypt(S, m)
  1. Group users in S into S’, a set of disjoint subsets
     - |S’| is sub-linear in |S|
  2. Generate a ciphertext c_i for each s_i in S’ (using anonymous IBE)
  3. Attach a tag t_i to each c_i (for efficient decryption at the receivers)
  4. Bundle all (t_i, c_i) components using one-time signature

$$\boxed{\sigma}\ \boxed{t_0}\ \boxed{t_1}\boxed{c_1}\ \cdots\ \boxed{t_l}\boxed{c_l}$$

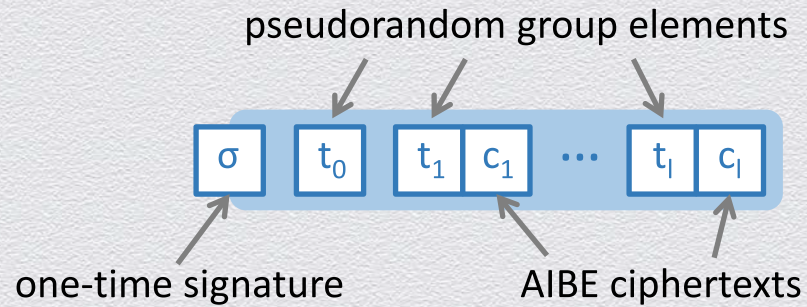
oABE Encryption in [FaPe12]

- Encrypt(S, m)
  1. Group users in S into S', a set of disjoint subsets
     - |S'| is sub-linear in |S|
  2. Generate a ciphertext c_i for each s_i in S' (using anonymous IBE)
  3. Attach a tag t_i to each c_i (for efficient decryption at the receivers)
  4. Bundle all (t_i, c_i) components using one-time signature

$$\boxed{\sigma}\ \boxed{t_0}\ \boxed{t_1 \mid c_1}\ \cdots\ \boxed{t_l \mid c_l}$$

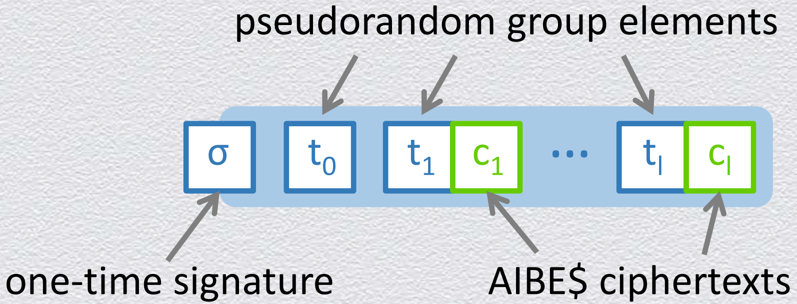
- Notice that ciphertexts have no header …
- … but still exhibit structure due to tags and signature
- Idea: Toward a BS construction, make these components pseudorandom

oABE with Pseudorandom Ciphertexts (oABE$) [This Work]



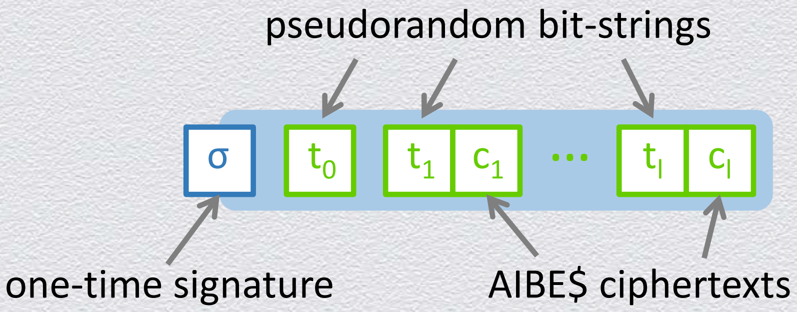
- How to make oABE ciphertexts pseudorandom?
  1. Replace the underlying AIBE with AIBE$ [AgBo09]
  2. Apply an entropy smoothing hash to group elements
  3. Replace one-time signature with a MAC (implemented via PRF)

oABE with Pseudorandom Ciphertexts (oABE$) [This Work]



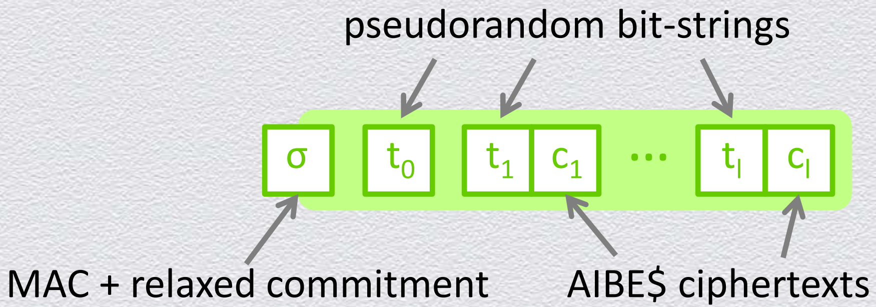
- How to make oABE ciphertexts pseudorandom?
  1. Replace the underlying AIBE with AIBE$ [AgBo09]
  2. Apply an entropy smoothing hash to group elements
  3. Replace one-time signature with a MAC (implemented via PRF)

oABE with Pseudorandom Ciphertexts (oABE$) [This Work]



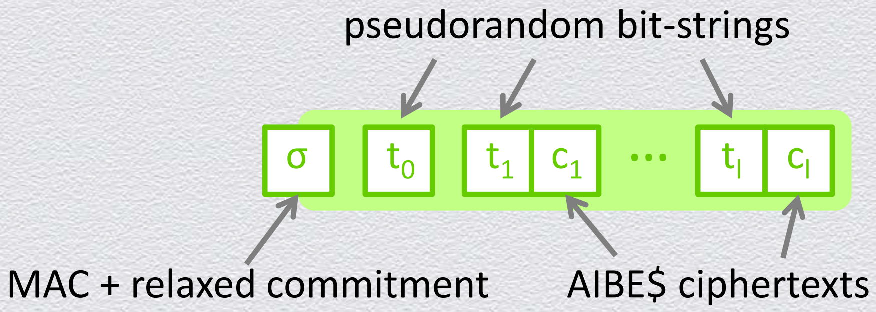
- How to make oABE ciphertexts pseudorandom?
  1. Replace the underlying AIBE with AIBE$ [AgBo09]
  2. Apply an entropy smoothing hash to group elements
  3. Replace one-time signature with a MAC (implemented via PRF)

oABE with Pseudorandom Ciphertexts (oABE$) [This Work]



- How to make oABE ciphertexts pseudorandom?
  1. Replace the underlying AIBE with AIBE$ [AgBo09]
  2. Apply an entropy smoothing hash to group elements
  3. Replace one-time signature with a MAC (implemented via PRF)

oABE with Pseudorandom Ciphertexts (oABE$) [This Work]



- How to make oABE ciphertexts pseudorandom?
  1. Replace the underlying AIBE with AIBE$ [AgBo09]
  2. Apply an entropy smoothing hash to group elements
  3. Replace one-time signature with a MAC (implemented via PRF)

Question: How to embed the MAC key in c_i's and still obtain CCA security?

Solution: Construct an encapsulation mechanism [DoKa05, BoKa05] with pseudorandom commitments

Comparison of BE Schemes with Anonymity Properties

Scheme	|PK|	|sk|	|c|	Security Model	Anonymity
BBW06	O(N)	O(1)	O(N-r)	Static, RO	Full
LPQ12	O(N)	O(1)	O(N-r)	Adaptive, Standard	Full
FaPe12a	O(N)	O(log N)	O(r log (n/r))	Adaptive, Standard	Outsider
FaPe12b	O(N log N)	O(N)	O(r)	Adaptive, Standard	Outsider
This Work	O(N)	O(log N)	O(r log (n/r))	Adaptive, Standard	Outsider

N: total number of users, r: number of revoked users

- Only oABE$ provides pseudorandom ciphertexts

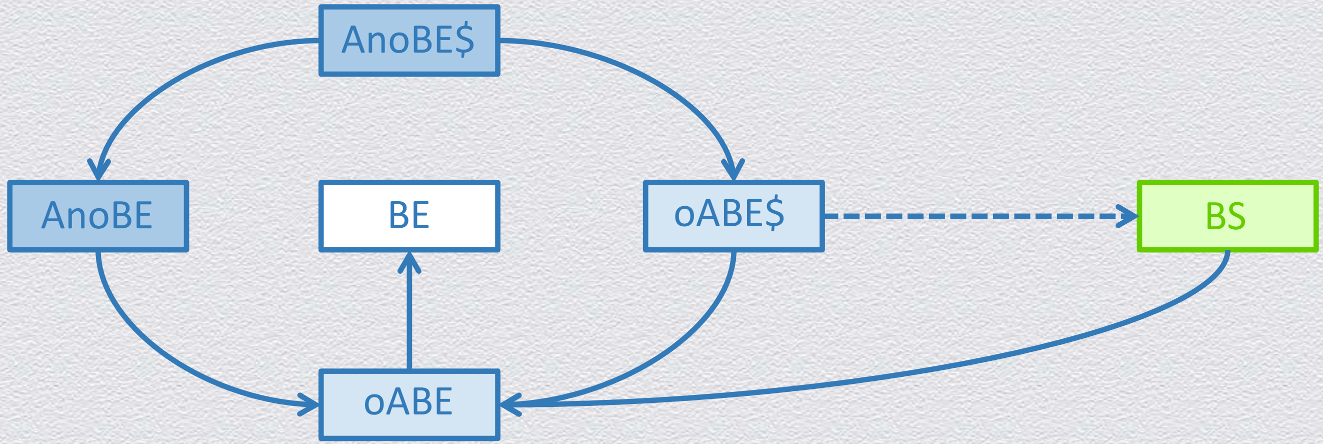
Our Construction of Broadcast Steganography

- Highlights
  - oABE$ + Encrypt-then-Embed = Broadcast Steganography
  - Our constructions have sub-linear stegotext length
  - For CCA security, requires stateless channel

- Constructions:
  1. BS-CHA
  2. BS-PDR-CCA
  3. BS-CCA

- Broadcast Steganography (BS)
- Constructions
- Summary

BE and Friends



Summary

- Initiated the study of Broadcast Steganography
  - A multi-recipient communication tool to plant undetectable messages in innocent-looking conversations
- Put forth sublinear constructions of broadcast steganography under a range of security notions
- In the process, devised efficient broadcast encryption schemes with pseudorandom ciphertexts and anonymity properties
  - Implementing CCA checks without imposing structure on broadcast ciphertexts required overcoming multiple technical hurdles

Practical Dual-Receiver Encryption

Soundness, Complete Non-malleability, and Applications

Sherman S.M. Chow ***Matthew Franklin*** ***Haibin Zhang***

Chinese University of Hong Kong
sherman@ie.cuhk.edu.hk

University of California, Davis
{franklin,hbzhang}@cs.ucdavis.edu

Our Contributions

- Reformizing and recasting Dual-Receiver Encryption

- Defining soundness notions

- Practical DREs with soundness in the CRS model

- Applications:
  1. Complete non-malleable encryption
  2. Plaintext-aware encryption
  3. More applicatons---PKE with plaintext equality test, off-the-record messaging, ...

- Practical combined encryption of DRE and PKE
- Complete non-malleable DRE

[Diament, Lee, Keromytis, Yung 2001]

What's Dual-Receiver Encryption?

- Original DLKY notion:

  A kind of PKE allowing a ciphertext to be decrypted into the same plaintext by two independent receivers.

[Diament, Lee, Keromytis, Yung 2001]

What's Dual-Receiver Encryption?

- Original DLKY notion:
  A kind of PKE allowing a ciphertext to be decrypted into the same plaintext by two independent receivers.

Receiver 1
(pk_1, sk_1)

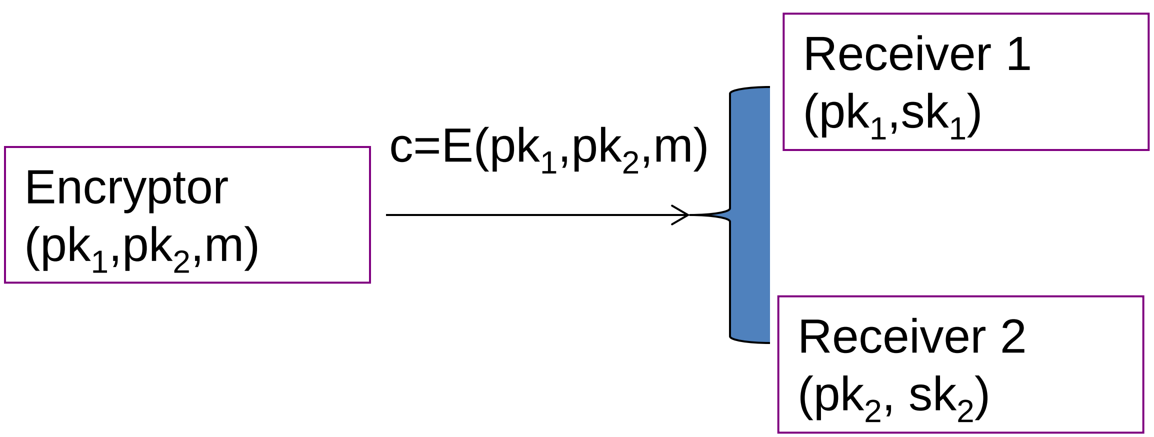
Encryptor
(pk_1, pk_2, m)

Receiver 2
(pk_2, sk_2)

[Diament, Lee, Keromytis, Yung 2001]

What's Dual-Receiver Encryption?

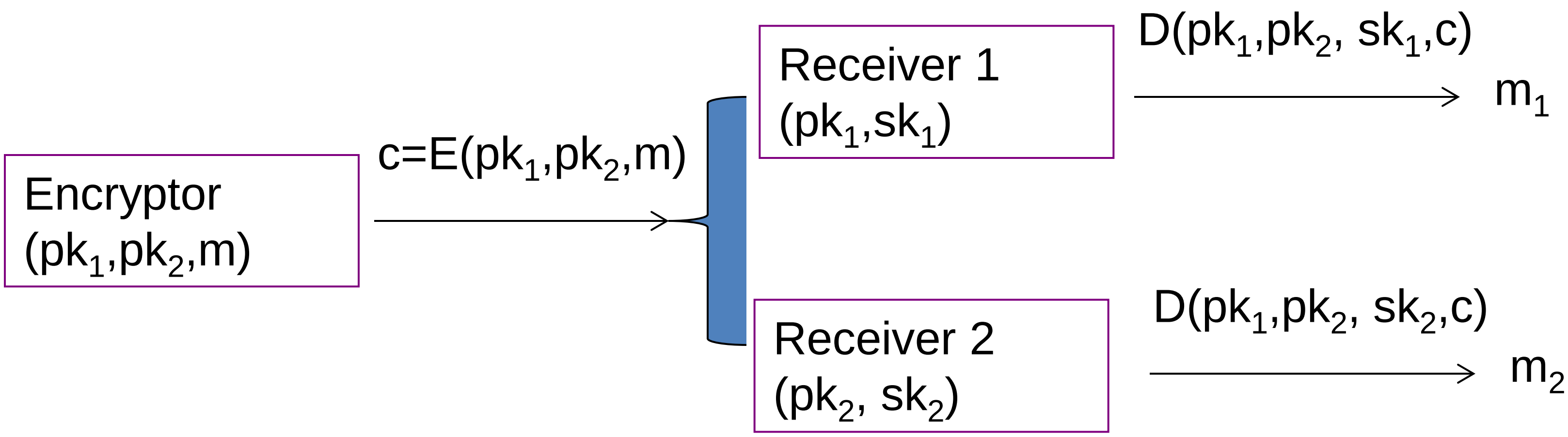
- Original DLKY notion:
  A kind of PKE allowing a ciphertext to be decrypted into the same plaintext by two independent receivers.



[Diament, Lee, Keromytis, Yung 2001]

What's Dual-Receiver Encryption?

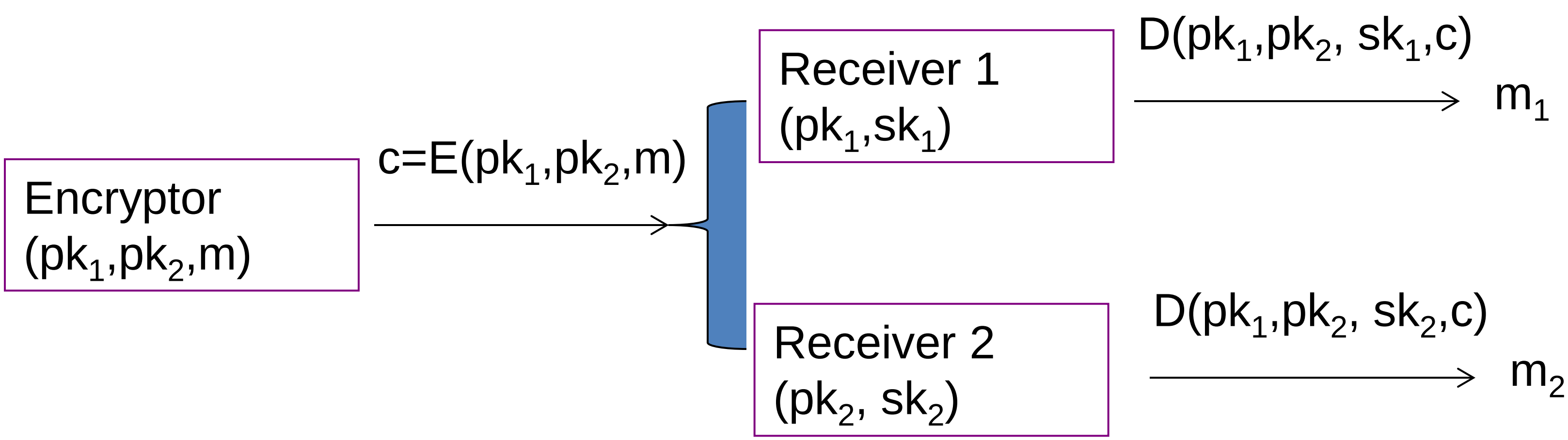
- Original DLKY notion:
  A kind of PKE allowing a ciphertext to be decrypted into the same plaintext by two independent receivers.



[Diament, Lee, Keromytis, Yung 2001]

What's Dual-Receiver Encryption?

- Original DLKY notion:
  A kind of PKE allowing a ciphertext to be decrypted into the same plaintext by two independent receivers.



Basic consistency: $m=m_1=m_2$

DRE: A Useful Primitive

- DLKY: constructing useful security puzzle.

[Diament, Lee, Keromytis, Yung 2001]

Extending the DLKY notion---Soundness

- What about a cheating encryptor?
- "Bad" example: E(pk1,pk2,m) = E(pk1, m)||E(pk2, m)
- Soundness goals:

  1. Ensure adversary cannot "cheat."

  2. Both receivers "know" the ciphertext can be decrypted to the same result.

Extending the DLKY notion-Soundness

- Formally:

$$
\begin{array}{l}
\textbf{Experiment } \mathbf{Exp}^{\mathrm{sound}}_{\mathcal{DRE},\mathcal{A}}(k) \\
\quad \mathsf{crs} \xleftarrow{\$} \mathsf{CGen}_{\mathrm{DRE}}(1^k) \\
\quad (pk_1, sk_1) \xleftarrow{\$} \mathsf{Gen}_{\mathrm{DRE}}(\mathsf{crs}); (pk_2, sk_2) \xleftarrow{\$} \mathsf{Gen}_{\mathrm{DRE}}(\mathsf{crs}) \\
\quad C \xleftarrow{\$} \mathcal{A}(\mathsf{crs}, pk_1, sk_1, pk_2, sk_2) \\
\quad \textbf{if } \mathsf{Dec}_{\mathrm{DRE}}(sk_1, C) \neq \mathsf{Dec}_{\mathrm{DRE}}(sk_2, C) \textbf{ then} \\
\quad \textbf{return } 1 \textbf{ else return } 0
\end{array}
$$

Extending the DLKY notion-Soundness

- Formally:

$$
\begin{array}{l}
\textbf{Experiment } \mathbf{Exp}^{\text{sound}}_{\mathcal{DRE},\mathcal{A}}(k) \\
\mathsf{crs} \xleftarrow{\$} \mathsf{CGen}_{\mathrm{DRE}}(1^k) \\
(pk_1, sk_1) \xleftarrow{\$} \mathsf{Gen}_{\mathrm{DRE}}(\mathsf{crs}); (pk_2, sk_2) \xleftarrow{\$} \mathsf{Gen}_{\mathrm{DRE}}(\mathsf{crs}) \\
C \xleftarrow{\$} \mathcal{A}(\mathsf{crs}, pk_1, sk_1, pk_2, sk_2) \\
\textbf{if } \mathsf{Dec}_{\mathrm{DRE}}(sk_1, C) \neq \mathsf{Dec}_{\mathrm{DRE}}(sk_2, C) \textbf{ then} \\
\textbf{return } 1 \textbf{ else return } 0
\end{array}
$$

$$
\mathbf{Adv}^{\text{sound}}_{\mathcal{DRE},\mathcal{A}}(k) = \Pr[\mathbf{Exp}^{\text{sound}}_{\mathcal{DRE},\mathcal{A}}(k) = 1].
$$

Extending the DLKY notion-Soundness

- Formally:

$$\textbf{Experiment } \mathbf{Exp}^{\text{sound}}_{\mathcal{DRE},\mathcal{A}}(k)$$
$$\mathsf{crs} \xleftarrow{\$} \mathsf{CGen}_{\mathrm{DRE}}(1^k)$$
$$(pk_1, sk_1) \xleftarrow{\$} \mathsf{Gen}_{\mathrm{DRE}}(\mathsf{crs}); (pk_2, sk_2) \xleftarrow{\$} \mathsf{Gen}_{\mathrm{DRE}}(\mathsf{crs})$$
$$C \xleftarrow{\$} \mathcal{A}(\mathsf{crs}, pk_1, sk_1, pk_2, sk_2)$$
$$\textbf{if } \mathsf{Dec}_{\mathrm{DRE}}(sk_1, C) \neq \mathsf{Dec}_{\mathrm{DRE}}(sk_2, C) \textbf{ then}$$
$$\textbf{return } 1 \textbf{ else return } 0$$

$$\mathbf{Adv}^{\text{sound}}_{\mathcal{DRE},\mathcal{A}}(k) = \Pr[\mathbf{Exp}^{\text{sound}}_{\mathcal{DRE},\mathcal{A}}(k) = 1].$$

We show DRE with soundness is even more useful.

Chosen Ciphertext Security of DRE

- DRE's soundness makes one of the two decryption oracles redundant.
- Formally:

$$\begin{array}{l}
\textbf{Experiment } \mathbf{Exp}^{\mathrm{cca}}_{\mathcal{DRE},\mathcal{A}}(k) \\
\quad \mathsf{crs} \xleftarrow{\$} \mathsf{CGen}_{\mathrm{DRE}}(1^k) \\
\quad (pk_1, sk_1) \xleftarrow{\$} \mathsf{Gen}_{\mathrm{DRE}}(\mathsf{crs});\ (pk_2, sk_2) \xleftarrow{\$} \mathsf{Gen}_{\mathrm{DRE}}(\mathsf{crs}) \\
\quad (M_0, M_1, \mathsf{s}) \xleftarrow{\$} \mathcal{A}^{\mathsf{Dec}_{\mathrm{DRE}}(sk_1,\cdot)}(\mathsf{find}, \mathsf{crs}, pk_1, pk_2) \\
\quad b \xleftarrow{\$} \{0,1\};\ C^* \xleftarrow{\$} \mathsf{Enc}_{\mathrm{DRE}}(\mathsf{crs}, pk_1, pk_2, M_b) \\
\quad b' \xleftarrow{\$} \mathcal{A}^{\mathsf{Dec}_{\mathrm{DRE}}(sk_1,\cdot)}(\mathsf{guess}, C^*, \mathsf{s}) \\
\quad \textbf{if } b' = b \textbf{ then return } 1 \textbf{ else return } 0
\end{array}$$

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{DRE},\mathcal{A}}(k) = \Pr[\mathbf{Exp}^{\mathrm{cca}}_{\mathcal{DRE},\mathcal{A}}(k) = 1] - 1/2.$$

Properties of a Desirable DRE

- Efficient; standard model; well-studied assumption
- Symmetry
- Public verifiability

Constructing DRE

- Previous constructions: either in ROM or rely on general and inefficient NIZK proofs

- We construct DRE in the CRS model.

  Our CRS is simply a benign bilinear group such that two receivers pick their keys from the group.

- We also construct DKEM

  DKEM=Dual-receiver Key Encapsulation Mechanism.

Practical DRE and DKEM from BDDH Assumption

- Basic ideas: Boneh and Boyen, Identity-based techniques

[Boneh and Boyen, 2004]

- DRE similar to: Kiltz tag-based encryption

[Kiltz, TCC 2006]

- DKEM similar to: Kiltz KEMs and BMW KEM

[Kiltz, TCC 2006][Kiltz, PKC 2007] [Boyen, Mei, and Waters, 2005]

Practical DRE from BDDH Assumption

$\mathsf{CGen}_{\mathrm{DRE}}(1^k)$	$\mathsf{Enc}_{\mathrm{DRE}}(\mathcal{BG}, pk_1, pk_2, M)$	$\mathsf{Dec}_{\mathrm{DRE}}(\mathcal{BG}, pk_1, pk_2, sk_1, C)$
$\textbf{return } \mathcal{BG}$	$(\mathsf{vk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{Gen}_{\mathrm{OT}}(1^k)$	$\textbf{parse } C \textbf{ as } (\mathsf{vk}, c, \pi_1, \pi_2, \phi, \sigma)$
$\mathsf{Gen}_{\mathrm{DRE}}(1^k, \mathcal{BG})$	$r \xleftarrow{\$} \mathbb{Z}_q^*;\ c \leftarrow g^r$	$\textbf{if } \mathsf{Vrf}_{\mathrm{OT}}(\mathsf{vk}, \sigma, (c, \pi_1, \pi_2, \phi)) \neq 1 \textbf{ or}$
$x_i, y_i \xleftarrow{\$} \mathbb{Z}_q^*$	$\pi_1 \leftarrow (u_1^{\mathsf{vk}} v_1)^r$	$e(g, \pi_1) \neq e(c, u_1^{\mathsf{vk}} v_1) \textbf{ or}$
$u_i \leftarrow g^{x_i};\ v_i \leftarrow g^{y_i}$	$\pi_2 \leftarrow (u_2^{\mathsf{vk}} v_2)^r$	$e(g, \pi_2) \neq e(c, u_2^{\mathsf{vk}} v_2)$
$pk_i \leftarrow (u_i, v_i)$	$\phi \leftarrow e(u_1, u_2)^r \cdot M$	$\textbf{return } \perp$
$sk_i \leftarrow x_i$	$\sigma \xleftarrow{\$} \mathsf{Sig}_{\mathrm{OT}}(\mathsf{sk}, (c, \pi_1, \pi_2, \phi))$	$M \leftarrow \phi \cdot e(c, u_2)^{-x_1}$
$\textbf{return } (pk_i, sk_i)$	$\textbf{return } C \leftarrow (\mathsf{vk}, c, \pi_1, \pi_2, \phi, \sigma)$	$\textbf{return } M$

- Efficient and practical
- Well-studied assumption---BDDH assumption
- Symmetric
- Public verifiable

Practical DKEM from BDDH Assumption

$\mathsf{CGen}_{\mathrm{DKEM}}(1^k)$	$\mathsf{Enc}_{\mathrm{DKEM}}(\mathcal{BG}, pk_1, pk_2)$	$\mathsf{Dec}_{\mathrm{DKEM}}(\mathcal{BG}, pk_1, pk_2, sk_1, C)$
return $\mathcal{BG}$	$r \xleftarrow{\$} \mathbb{Z}_q^*;\ c \leftarrow g^r$	**parse** C **as** (c, π_1, π_2)
$\mathsf{Gen}_{\mathrm{DKEM}}(1^k, \mathcal{BG})\ i \in \{1,2\}$	$t \leftarrow \mathsf{TCR}(c)$	$t \leftarrow \mathsf{TCR}(c)$
$x_i, y_i \xleftarrow{\$} \mathbb{Z}_q^*$	$\pi_1 \leftarrow (u_1^t v_1)^r$	**if** $e(g, \pi_1) \neq e(c, u_1^t v_1)$ **or**
$u_i \leftarrow g^{x_i};\ v_i \leftarrow g^{y_i}$	$\pi_2 \leftarrow (u_2^t v_2)^r$	$e(g, \pi_2) \neq e(c, u_2^t v_2)$
$pk_i \leftarrow (u_i, v_i)$	$K \leftarrow e(u_1, u_2)^r$	**return** $\perp$
$sk_i \leftarrow x_i$	$C \leftarrow (c, \pi_1, \pi_2)$	$K \leftarrow e(c, u_2)^{x_1}$
return (pk_i, sk_i)	**return** (C, K)	**return** K

Plaintext-Aware (PA) Encryption via Registration

- Plaintext aware encryption

1. "Any adversary can decrypt any ciphertext that it creates"

2. PA+IND-CPA-->IND-CCA2

3. PA encryption in the standard model --- difficult to analyze.

Plaintext-Aware (PA) Encryption via Registration

PA via registration --- "Any adversary can decrypt any ciphertext it creates, as long as the adversary registered its sending key."

[Herzog, Liscov, Micali (HLM) 2003]

HLM is relatively simple but relies on generic NIZK proofs.

Plaintext Aware Encryption via Registration from DRE

- General transformation:
  Given a DRE with (pk1,sk1) and (pk2,sk2),

  pk1 is the sender and pk2 is the receiver;
  pk1 further runs a zero-knowledge PoK of its secret key.

- Efficient; symmetric; general; simple to analyze.

Complete Non-Malleable (CNM) PKE from DRE

- CNM----another strong notion than IND-CCA2/NM-CCA2.

[Fischlin 2005] [Ventre and Visconti 2008]

- CNM prohibits adversary from computing encrypted ciphertext of related plaintext even with adverserial public keys.

- DRE with soundness implies CNM PKE in the CRS model.

- The transformation is even simpler:

Given a DRE with (pk1,sk1) (pk2,sk2).

crs---pk1, PKE's (pk,sk)=DRE's (pk2,sk2).

Public key encryption with equality test (PET) from DRE

- Two types of PET:

- 1. Probabilistic PKE with equality test:
  one-way CCA [Yang, Tan, Huang, Wong 2010]
  a stronger notion (still weak than one for PKE) [Lu, Zhang, Lin 2012]

- 2. e-voting and verifiable dual encryption (chosen-plaintext attack model):
  e.g.,[Jakobsson and Juels 2000]
  [Zhou, Marsh, Schneider, Redz 2005]

Our DRE with soundness strengthens two types of PET.

Off-the-record messaging with stronger undeniability from DRE

- Off-the-record messaging (OTR) protocol.

[Borisov, Goldberg, Brewer, 2000]

- DKSW proposed stronger notion for undenaiability. The bottleneck is jus the efficiency of DRE.

[Dodis, Katz, Smith, and Walfish 2009]

- OTR made practical with our DREs.

Other Applications

- Key exchange protocols.

[Suzuki and Yoneyama 2013]

[Purushothama and Amberker 2013]

Combined Encryption of DRE and PKE

- Combined encryption of DRE and PKE without key separation.

$\mathsf{CGen}(1^k)$
 return $\mathcal{BG}$
$\mathsf{Gen}_{\mathrm{COM}}(1^k, \mathcal{BG})$
 $x_i, y_i \xleftarrow{\$} \mathbb{Z}_q^*$
 $u_i \leftarrow g^{x_i};\ v_i \leftarrow g^{y_i}$
 $w_i \leftarrow g^{z_i}$
 $pk_i \leftarrow (u_i, v_i, w_i)$
 $sk_i \leftarrow x_i$
 return (pk_i, sk_i)

$\mathsf{Enc}_{\mathrm{DRE}}(\mathcal{BG}, pk_1, pk_2, M)$
 $(\mathsf{vk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{Gen}_{\mathrm{OT}}(1^k)$
 $r \xleftarrow{\$} \mathbb{Z}_q^*$
 $c \leftarrow g^r$
 $\pi_1 \leftarrow (u_1^{\mathsf{vk}} v_1)^r$
 $\pi_2 \leftarrow (u_2^{\mathsf{vk}} v_2)^r$
 $\phi \leftarrow e(u_1, u_2)^r \cdot M$
 $\sigma \xleftarrow{\$} \mathsf{Sig}_{\mathrm{OT}}(\mathsf{sk}, (c, \pi_1, \pi_2, \phi))$
 return $C \leftarrow (\mathsf{vk}, c, \pi_1, \pi_2, \phi, \sigma)$

$\mathsf{Dec}_{\mathrm{DRE}}(\mathcal{BG}, pk_1, pk_2, sk_1, C)$
 parse C **as** $(\mathsf{vk}, c, \pi_1, \pi_2, \phi, \sigma)$
 if $\mathsf{Vrf}_{\mathrm{OT}}(\mathsf{vk}, \sigma, (c, \pi_1, \pi_2, \phi)) \neq 1$ **or**
  $e(g, \pi_1) \neq e(c, u_1^{\mathsf{vk}} v_1)$ **or**
  $e(g, \pi_2) \neq e(c, u_2^{\mathsf{vk}} v_2)$
 return $\perp$
 $M \leftarrow \phi \cdot e(c, u_2)^{-x_1}$
 return M

$\mathsf{Enc}_{\mathrm{PKE}}(\mathcal{BG}, pk_1, M)$
 $(\mathsf{vk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{Gen}_{\mathrm{OT}}(1^k)$
 $r \xleftarrow{\$} \mathbb{Z}_q^*;\ c \leftarrow g^r$
 $\pi \leftarrow (u_1^{\mathsf{vk}} v_1)^r$
 $\phi \leftarrow e(u_1, w_1)^r \cdot M$
 $\sigma \xleftarrow{\$} \mathsf{Sig}_{\mathrm{OT}}(\mathsf{sk}, (c, \pi, \phi))$
 return $C \leftarrow (\mathsf{vk}, c, \pi, \phi, \sigma)$

$\mathsf{Dec}_{\mathrm{PKE}}(\mathcal{BG}, pk_1, sk_1, C)$
 parse C **as** $(\mathsf{vk}, c, \pi, \phi, \sigma)$
 if $\mathsf{Vrf}_{\mathrm{OT}}(\mathsf{vk}, \sigma, (c, \pi, \phi)) \neq 1$ **or**
  $e(g, \pi) \neq e(c, u_1^{\mathsf{vk}} v_1)$ **then**
 return $\perp$
 $M \leftarrow \phi \cdot e(c, w_1)^{-x_1}$
 return M

Complete Non-Malleable DRE

- Motivated by
  1. same reason as CNM PKE---stonger security for DRE
  2. stronger security for PETs
  3. dual-receiver non-malleable commitment scheme

Paradigms for CNM-DRE (1): Groth-Sahai Proof System

- Naor-Yung Paradigm and Groth-Sahai Proof system

[Naor, Yung, 1990] [Groth, Sahai, 2008]

$\mathsf{CGen}_{\mathrm{DRE}}(1^k)$	$\mathsf{Enc}_{\mathrm{DRE}}(\mathsf{crs}, pk_1, pk_2, m)$	$\mathsf{Dec}_{\mathrm{DRE}}(\mathsf{crs}, pk_1, pk_2, sk_1, C)$
$\textbf{return}\ \mathsf{crs} \xleftarrow{\$} \mathsf{CGen}(1^k)$	$c_1 \leftarrow \mathsf{Enc}(pk_1, m; r_1)$	$\textbf{parse}\ C\ \textbf{as}\ (c_1, c_2, \pi)$
	$c_2 \leftarrow \mathsf{Enc}(pk_2, m; r_2)$	$\textbf{if}\ \mathsf{V}(\mathsf{crs}, c_1, c_2, pk_1, pk_2, \pi) \neq 1$
$\mathsf{Gen}_{\mathrm{DRE}}(1^k)\quad i \in \{1,2\}$	$\pi \xleftarrow{\$} \mathsf{P}(\mathsf{crs}, (c_1, c_2, pk_1, pk_2), (m, r_1, r_2))$	$\quad \textbf{return}\ \perp$
$(pk_i, sk_i) \xleftarrow{\$} \mathsf{Gen}(1^k)$	$c \leftarrow (c_1, c_2, \pi)$	$m \leftarrow \mathsf{Dec}(c_1, pk_1, sk_1)$
$\textbf{return}\ (pk_i, sk_i)$	$\textbf{return}\ c$	$\textbf{return}\ m$

- (P,V) is simulation-sound and simulation-sound extractable NIZK proof of knowledge proof system
- can be realized via Groth-Sahai proof system
- SXDH and DLIN assumptions

Paradigms for CNM-DRE (2): Lossy Trapdoor Functions

- Lossy trapdoor functions (DDH, LWE, and CR assumptions)

[Peikert, Waters2008][Freeman, Goldreich, Kiltz, Segev2010]

$\mathsf{CGen}_{\mathrm{DRE}}(1^k)$
- $b_0 \xleftarrow{\$} \{0,1\}^n$
- $(s_0, t_0) \xleftarrow{\$} \mathcal{S}_{abo}(1^k, b_0)$
- $h \xleftarrow{\$} \mathcal{H}$
- **return** $\mathsf{crs} \leftarrow (s_0, h)$

$\mathsf{Gen}_{\mathrm{DRE}}(1^k) \quad i \in \{1,2\}$
- $(s_i, t_i) \xleftarrow{\$} \mathcal{S}(1^k, 1)$
- **return** (s_i, t_i)

$\mathsf{Dec}_{\mathrm{DRE}}(\mathsf{crs}, s_1, s_2, t_1, C)$
- **parse** C **as** $(C_1, C_2, C_3, C_4, pk_1, pk_2, \sigma)$
- **if** $\mathsf{Vrf}_{\mathrm{OT}}(\mathsf{vk}, \sigma, (C_1, C_2, C_3, C_4, pk_1, pk_2)) \neq 1$ **then**
  - **return** $\perp$
- $r \leftarrow \mathcal{F}^{-1}(t_1, C_1)$
- **if** $C_2 \neq \mathcal{F}(s_2, r)$ **or** $C_3 \neq \mathcal{F}(s_0, r)$ **then**
  - **return** $\perp$
- $m \leftarrow C_4 \oplus \mathsf{H}_h(r)$
- **return** m

$\mathsf{Enc}_{\mathrm{DRE}}(\mathsf{crs}, s_1, s_2, m; r)$
- $(\mathsf{vk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{Gen}_{\mathrm{OT}}(1^k)$
- $r \xleftarrow{\$} \{0,1\}^n$
- $C_1 \leftarrow \mathcal{F}(s_1, r)$
- $C_2 \leftarrow \mathcal{F}(s_2, r)$
- $C_3 \leftarrow \mathcal{G}_{abo}(s_0, \mathsf{vk}, r)$
- $C_4 \leftarrow M \oplus \mathsf{H}_h(r)$
- $\sigma \xleftarrow{\$} \mathsf{Sig}_{\mathrm{OT}}(\mathsf{sk}, (C_1, C_2, C_3, C_4, pk_1, pk_2))$
- **return** $C \leftarrow (\mathsf{vk}, C_1, C_2, C_3, C_4, \sigma)$

Thank you!