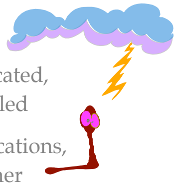
Friday

Sources

- G. Ateniese, J. Camenish, and B. de Medeiros, "Untraceable RFIDs via Insubvertible Encryption", ACM CCS 2005, and references therein.
- Many thanks to Breno for providing most of the next slides.

- A scheme for RFID untraceability
  - It has applications in Mixnets, secure shuffling (e-voting), and any other setting with oblivious re-encryptors
- A new, unlinkably randomizable certification scheme.
  - Wider application in privacy protocols. (E.g., group signatures)
- Provable security in the UC framework by reduction in the standard model to new cryptographic assumptions

Solution 1: Kill



- Disable it (after the point-of-sale)
  - If kill-operation is not authenticated, tags could be maliciously disabled
- Prevents after-point-of-sale applications, such as automated home, consumer experience customization
- Does not provide protection against cloning unless reader authentication is employed

Solution 2: Encrypt contents

- Provides confidentiality of contents for post-sale applications
- Does not require reader authentication, may use tag as passive device
- Does not provide protection against tracking and/or profiling

Solution 3: Re-encrypt

- Tag contents are (non-deterministically) re-encrypted after each reading.
- Permits post-sale applications of RFID, but only non-critical ones:
  - Tag can be cloned, if it does not authenticate reads.
  - Tag can be obliterated, if it does not authenticate writes.

Oblivious re-encryptors

- Higher privacy achieved when reader/writers are abundant
  - For instance, user home devices
- If public key encryption used, no nee for tamper-proof RFID-RW.
- Achievable w/ passive tags

Re-encryption w/ multiple issuers

- If single issuer uses the platform, re-encryption is sufficient.
- If multiple issuers are used, problems arise:
  - If the identity of the issuer is stored in plaintext in the tag, then profiling is possible
- No need to store issuers identities if *universal re-encryption* is used. However, that enables *direct tracking* by exploitation of *hidden channels*.

Elgamal re-encryption

- p; a prime
- g; generator of a prime-order cryptographic group $\mathbf{G}$
- Public key: y
- Private key: x; $y = g^x$
- Encrypt: $m \rightarrow (A, B) = (g^r, m\, y^r)$
- Re-encrypt: $(A, B) \rightarrow (g^s A, y^s B) = (g^{r+s}, m\, y^{r+s})$

Key-private re-encryption

- Public keys may remain confidential
- System parameter: p, a prime
- Public key: (g, y) in group **G** of order p
- Encrypt:
  $(g, y, m) \rightarrow (A, B, C, D) = (g^s, y^s, g^r, my^r)$
- Re-encrypt:
  $(A, B, C, D) \rightarrow (A^w, B^w, A^zC, B^zD)$

Universal re-encryption issues

- Key-private re-encryption was introduced by Golle, Jakobsson, Juels, and Syverson in CT-RSA 2004. Proposed use for non-critical RFID applications providing privacy.
  - Hidden channels return! If the tracker obliterates the encryption to use his public key, re-encryption preserves the attacker's values.
- Problem: Cannot tell between legitimate public keys (authorized issuers) and others

Plugging hidden channels

- To prevent unauthorized use a certification scheme is needed.
- Certificates could be placed alongside with public keys on the tags.
- Certificates could break privacy, unless they can be randomized.
- Difficulty: How to create simultaneously randomizable and unforgeable certificates.

Insubvertible encryption

- Camenisch and Lysyanskaya (CRYPTO 2004) proposed a randomizable (via exponentiation) signature scheme.
  - Could it be used to sign public keys, as randomizable certificates?
- Not directly.
  - The randomized CL signatures verify against the original message.
  - Need modification if the message (public key) is to be simultaneously randomized.

- CL signature requires elliptic curve groups with an efficient algorithm for deciding the DH problem.
  - Given (g, g_1, g_2, g_3) in a cyclic group G, decide if there is an a such that

    $g_1 = g^a$, and $g_3 = g_2^a$
- In such groups, the (plain) Elgamal cryptosystem is not secure, and secure modifications of Elgamal are not universally re-encryptable.

- Two paired groups G, Γ such that the Co-DDH problem is efficiently solvable:
- Given (g, h, γ, η), is there a such that

  $g = h^a$, and $\eta = \gamma^a$
- Yet the DDH problem in groups G, Γ is computationally infeasible.

- M. Scott, *ID-based key exchange and remote log-in w/ simple token and PIN number.* (Incorporated the MNT curves in MIRACL library.)
- Boneh, Boyen, and Shacham. *Short group signatures.*
- L. Ballard, M. Green, BdM, and F. Monrose. *Correlation-resistant Storage.*
- E. Verheul. *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems.*
- S. Galbraith and V. Rotger. *Easy-Decision Diffie-Hellman groups.*

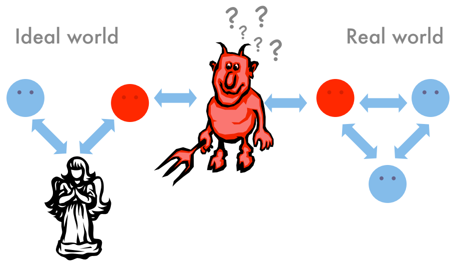
Scheme description

- Elliptic curve E over F_q, subgroups G in $E(F_q)$, and Γ in $E(F_{q^\alpha})$, of prime order p.
- Pairing e: $G \times \Gamma \rightarrow G_T$
- Generating public keys:
  - CA: $(\Sigma, T) \leftarrow (\gamma^s, \gamma^t)$ in group Γ
  - User: $Y \leftarrow g^x$ in group G

- Certifying the public key:
  - $(a_1, a_2, a_3, a_4, a_5) \leftarrow (a, a^t, a^{s+sxt}, a^x, a^{tx})$
- Tag contents:
  - $(a_1, a_2, a_3, a_4, a_5, b_1 = a^r, b_2 = m\, a^{xr})$
- Randomizing: Generate random s, v:
  - $(a_1^s, a_2^s, a_3^s, a_4^s, a_5^s, b_1 a_1^v, b_2 a_4^v)$

- XDH setting implies that Elgamal is semantically secure and key-private.
- Efficient computability of mixed decisional DH makes the modified CL signature verifiable after randomization, while *Strong LRSW assumption* (GM proof) gives unforgeability.
- Tag stores randomized certificate + public key
- Attacker needs certificate to substitute keys into a tag.

UC framework



THANK YOU!!! :-)