Computational soundness of formal encryption in the presence of key cycles, in the plain model

Peeter Laud
peeter@cyber.ee
http://www.cs.ut.ee/~peeter_l

Cybernetica AS & Tartu University

Reconciling two views of cryptography...

- A paper by Martín Abadi and Phillip Rogaway. Year: 2000.
- Theorem: Let
  - E_1 and E_2 be two formal expressions.
  - $[\![E_1]\!]$ and $[\![E_2]\!]$ be families of probability distributions over bit-strings associated to them.

  If $E_1 \cong E_2$ then $[\![E_1]\!] \approx [\![E_2]\!]$.

Condition [Abadi and Rogaway, 2000]:

No encryption cycles in E_1 or E_2

Reconciling two views of cryptography...

- A paper by Martín Abadi and Phillip Rogaway. Year: 2000.
- Theorem: Let
  - E_1 and E_2 be two formal expressions.
  - $[\![E_1]\!]$ and $[\![E_2]\!]$ be families of probability distributions over bit-strings associated to them.

  If $E_1 \cong E_2$ then $[\![E_1]\!] \approx [\![E_2]\!]$.

Condition [Black, Rogaway and Shrimpton, 2002]:

Encryption cycles OK, but need the random oracle

Reconciling two views of cryptography. . .

- A paper by Martín Abadi and Phillip Rogaway. Year: 2000.
- Theorem: Let
  - E_1 and E_2 be two formal expressions.
  - $[\![E_1]\!]$ and $[\![E_2]\!]$ be families of probability distributions over bit-strings associated to them.

  If $E_1 \cong E_2$ then $[\![E_1]\!] \approx [\![E_2]\!]$.

Condition inspired from [Boneh, Halevi, Hamburg, Ostrovsky, 2008]:

no condition

Formal expressions

$$
\begin{array}{rcll}
E & ::= & C & \text{constants} \\
 & | & K_j^- & \text{secret keys, } 1 \le j \le n \\
 & | & K_j^+ & \text{public keys} \\
 & | & (E_1, E_2) & \text{pairs} \\
 & | & \{E\}^R_{K_j^+} & \text{public-key encryptions}
\end{array}
$$

R — formal randomness to distinguish

$(\{E\}^R_{K^+}, \{E\}^R_{K^+})$ and $(\{E\}^R_{K^+}, \{E\}^{R'}_{K^+})$

Formal expressions
No inherent representation as bit-strings
There's only syntax

Computational interpretation

- $[\![E]\!]$ — a family (indexed by the security parameter η) of probability distributions over sequences of elements in $\mathbb{G}$.

Use an ElGamal-like PK encryption scheme $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ over $\mathbb{G}$.

Initialize: $(\tau_\eta(K_j^-), \tau_\eta(K_j^+)) \leftarrow \mathcal{G}(1^\eta)$ for each j

$$\begin{aligned}
[\![C]\!]_\eta &= \text{“const”} \| C \\
[\![K_j^+]\!]_\eta &= \text{“pk”} \| \tau_\eta(K_j^+) \\
[\![K_j^-]\!]_\eta &= \text{“sk”} \| \tau_\eta(K_j^-) \\
[\![(E_1, E_2)]\!]_\eta &= \text{“pair”} \| \, |E_1| \, \| [\![E_1]\!]_\eta \| [\![E_2]\!]_\eta \\
[\![\{E\}^R_{K_j^+}]\!]_\eta &= \text{“ct”} \| \mathcal{E}(1^\eta, \tau_\eta(K_j^+), [\![E]\!]_\eta)
\end{aligned}$$

$\mathcal{E}(b_1 \| \cdots \| b_k) \triangleq \mathcal{E}(b_1) \| \cdots \| \mathcal{E}(b_k)$. For each E, compute $[\![E]\!]_\eta$ at most once.

Patterns of expressions

Analyze the formal expression E:

- Given (E_1, E_2), can obtain E_1 and E_2.
- Given $\{E\}^R_{K_j^+}$ and K_j^-, can obtain E.

Let $Keys(E)$ be the set of secret keys that can be obtained from E.

Example: Let E be

$$K_1^-, \{K_2^-, C_1\}^{R_1}_{K_1^+}, \{C_3, K_1^-, K_2^+\}^{R_2}_{K_3^+}, \{C_2, K_3^+, \{C_4\}^{R_4}_{K_4^+}\}^{R_3}_{K_2^+}$$

Replace submessages $\{E'\}^R_{K_j^+}$, where $K_j^- \notin Keys(E)$, with undecryptables ${}_l\square^R_j$, where $l = |E'|$:

$$K_1^-, \{K_2^-, C_1\}^{R_1}_{K_1^+}, \qquad {}_{l_1}\square^{R_2}_{K_3^+}, \qquad \{C_2, K_3^+, {}_{l_2}\square^{R_4}_{K_4^+}\}^{R_3}_{K_2^+}$$

Theorem [Abadi&Rogaway, 2000]

If patterns of E_1 and E_2 are equal *modulo* renaming of formal keys and randomnesses, then $[\![E_1]\!] \approx [\![E_2]\!]$.

Caveat: E_1 and E_2 may not contain encryption cycles.

Proof sketch: Define also $[\![_l\Box^R_K]\!]$ as the encryption of a constant string. Show that $[\![E]\!] \approx [\![pattern(E)]\!]$.

Boneh-Halevi-Hamburg-Ostrovsky cryptosystem

Secret key $(a_1, \ldots, a_\ell) \in \mathbb{G}^\ell$, public key $(g_1, \ldots, g_\ell, h) \in \mathbb{G}^{\ell+1}$
Satisfy certain properties.

To encrypt $m \in \mathbb{G}$, generate random $r \in \mathbb{Z}_{|\mathbb{G}|}$. Ciphertext is $(g_1^r, \ldots, g_\ell^r, h^r m)$.

Secure wrt. the following experiment (adversary guesses the bit b):

- Generate pairs (sk_i, pk_i) where $1 \leq i \leq n$, $sk_i = (a_{i1}, \ldots, a_{i\ell})$, $pk_i = (g_{i1}, \ldots, g_{i\ell}, h_i)$. Give $pk_1, \ldots, pk_n$ to the adversary.
- Repeat: the adversary submits $\boxed{j} \in \{1, \ldots, n\}$ and $\boxed{u_{11}, \ldots, u_{n\ell}, v} \in \mathbb{G}$. Let $y = a_{11}^{u_{11}} \cdots a_{n\ell}^{u_{n\ell}} \cdot v$.
  If $b = 0$ return $\mathcal{E}(pk_j, y)$. If $b = 1$ return $\mathcal{E}(pk_j, 1_{\mathbb{G}})$.

IND-CPA even in the presence of a limited form of key-dependent messages. (affine dependencies from secret keys)

AR, BHHO, and encryption cycles

- BHHO cryptosystem does not provide general KDM-security.
- AR-interpretation does not use arbitrary functions on secret keys.

$$
\begin{aligned}
[\![C]\!]_\eta &= \text{“const”} \,\|C \\
[\![K_j^+]\!]_\eta &= \text{“pk”} \,\|\tau_\eta(K_j^+) \\
[\![K_j^-]\!]_\eta &= \text{“sk”} \,\|\tau_\eta(K_j^-) \\
[\![(E_1, E_2)]\!]_\eta &= \text{“pair”} \,\| \,|E_1|\, \|[\![E_1]\!]_\eta \|[\![E_2]\!]_\eta \\
[\![\{E\}_{K_j^+}^R]\!]_\eta &= \text{“ct”} \,\|\mathcal{E}(1^\eta, \tau_\eta(K_j^+), [\![E]\!]_\eta) \\
[\![{}_l\Box_{K_j^+}^R]\!]_\eta &= \text{“ct”} \,\|\mathcal{E}(1^\eta, \tau_\eta(K_j^+), 1_{\mathbb{G}})^{l \text{ times}}
\end{aligned}
$$

All blocks are affinely computed from secret keys.

AR, BHHO, and encryption cycles

- BHHO cryptosystem does not provide general KDM-security.
- AR-interpretation does not use arbitrary functions on secret keys.

$$
\begin{aligned}
[\![C]\!]_\eta &= \text{“const”} \| C \\
[\![K_j^+]\!]_\eta &= \text{“pk”} \| g_{j1} \| \cdots \| g_{j\ell} \| h_j \\
[\![K_j^-]\!]_\eta &= \text{“sk”} \| a_{j1} \| \cdots \| a_{j\ell} \\
[\![(E_1, E_2)]\!]_\eta &= \text{“pair”} \| \, |E_1| \, \| [\![E_1]\!]_\eta \| [\![E_2]\!]_\eta \\
[\![\{E\}^R_{K_j^+}]\!]_\eta &= \text{“ct”} \| (g_{j1}^r \| \cdots \| g_{j\ell}^r \| b \cdot h_j^r)^{\text{for all blocks } b \text{ of } [\![E]\!]_\eta} \\
[\![{}_l\square^R_{K_j^+}]\!]_\eta &= \text{“ct”} \| (g_1^r \| \cdots \| g_\ell^r \| h^r)^{l \text{ times}}
\end{aligned}
$$

AR, BHHO, and encryption cycles

- BHHO cryptosystem does not provide general KDM-security.
- AR-interpretation does not use arbitrary functions on secret keys.

$$[\![C]\!]_\eta = \text{“const”} \| C$$

$$[\![K_j^+]\!]_\eta = \text{“pk”} \| g_{j1} \| \cdots \| g_{j\ell} \| h_j$$

$$[\![K_j^-]\!]_\eta = \text{“sk”} \| a_{j1} \| \cdots \| a_{j\ell}$$

$$[\![(E_1, E_2)]\!]_\eta = \text{“pair”} \| \, |E_1| \, \| [\![E_1]\!]_\eta \| [\![E_2]\!]_\eta$$

$$[\![\{E\}_{K_j^+}^R]\!]_\eta = \text{“ct”} \| (g_{j1}^r \| \cdots \| g_{j\ell}^r \| b \cdot h_j^r)^{\text{for all blocks } b \text{ of } [\![E]\!]_\eta}$$

$$[\![{}_l\Box_{K_j^+}^R]\!]_\eta = \text{“ct”} \| (g_1^r \| \cdots \| g_\ell^r \| h^r)^{l \text{ times}}$$

constants induction base induction step

Multiplication preserves affineness

Conclusions

- Issue with encryption cycles not yet solved in the plain model.
  - One can consider more general functions applied to the secret keys.
- In modeling cryptographic protocols, more general functions are often not considered.