Probing the security landscape for authenticated key establishment protocols

Alekseev Evgeny, Kyazhin Sergey

CryptoPro LLC

CRYPTOPRO

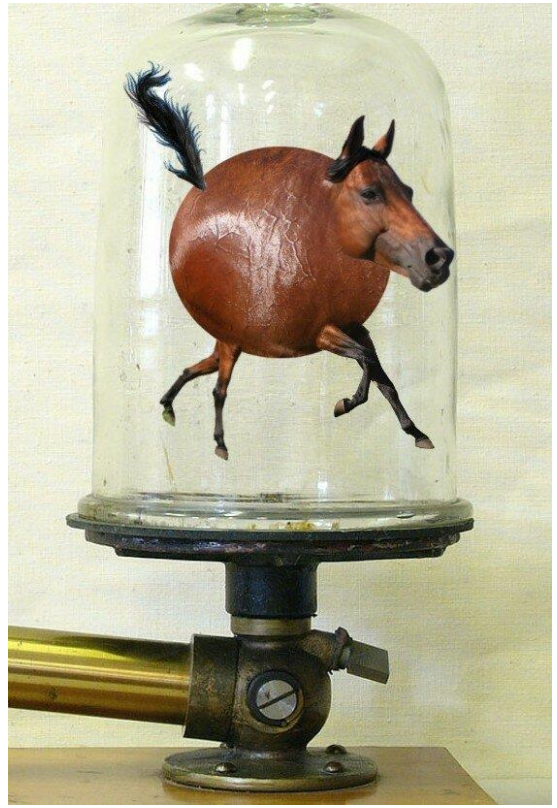
2023 CTCRYPT

Security Models in Cryptography

Cryptanalysis steps:

1) Identify a relevant security model
2) Describe the model formally
3) Get security estimation within a formal model

Step 1 is based on expert experience



Phong Q. Nguyen:

«There are a lot of similarities between cryptology and physics.
Both use a lot of mathematics, but neither is part of mathematics.»

Security Models in Cryptography

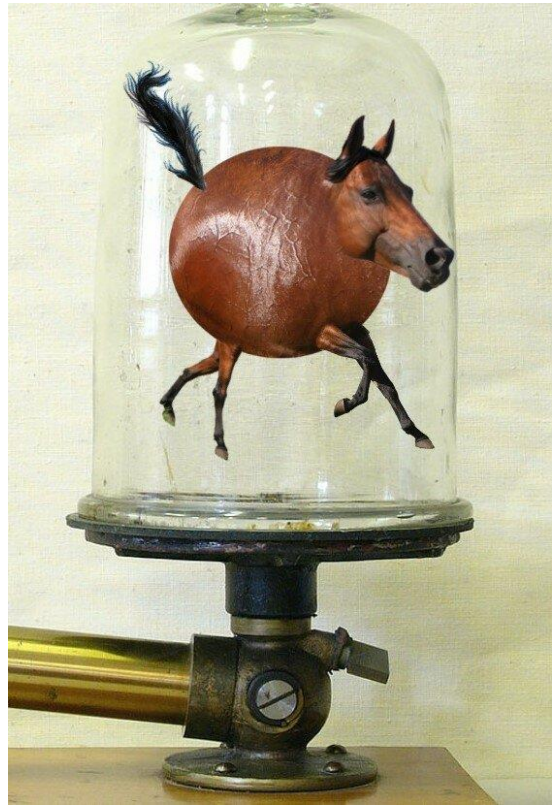
Cryptanalysis steps:

1) Identify a relevant security model
2) Describe the model formally
3) Get security estimation within a formal model

Step 1 is based on expert experience

Phong Q. Nguyen:

«There are a lot of similarities between cryptology and physics.
Both use a lot of mathematics, but neither is part of mathematics.»



Threats and Adversary Capabilities

Security model:

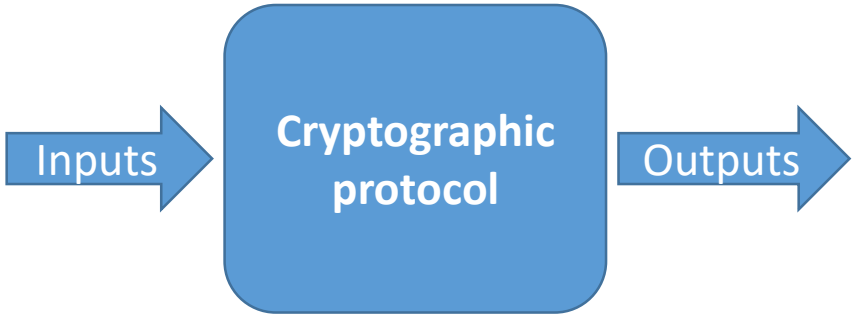
- Threats — *what the adversary wants*
- Adversary capabilities — *what the adversary can*
- Adversary resources — quantitative characteristics of the adversary capabilities

Security landscape for cryptosystem is a set of possible security models.

We propose 7 steps to systematically form security landscape.

Security Landscape

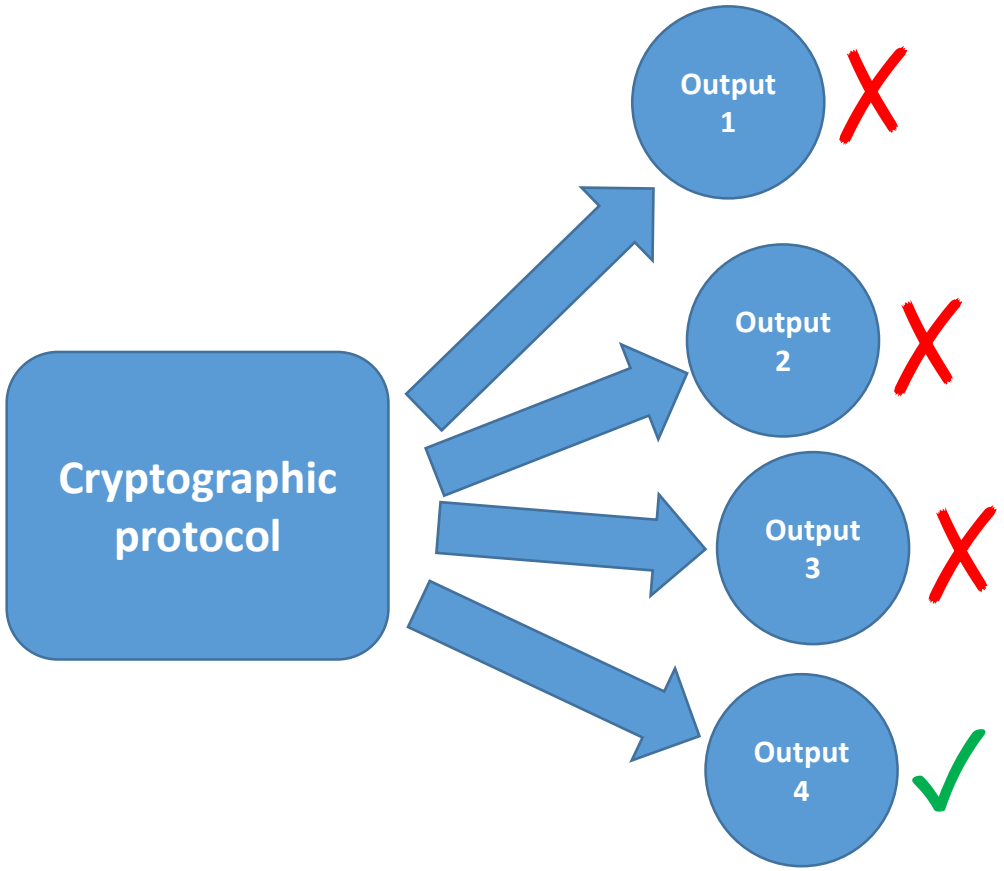
Step 1. Define the interface



Security Landscape

Step 1. Define the interface

Step 2. Determine “(ab)normal” outputs

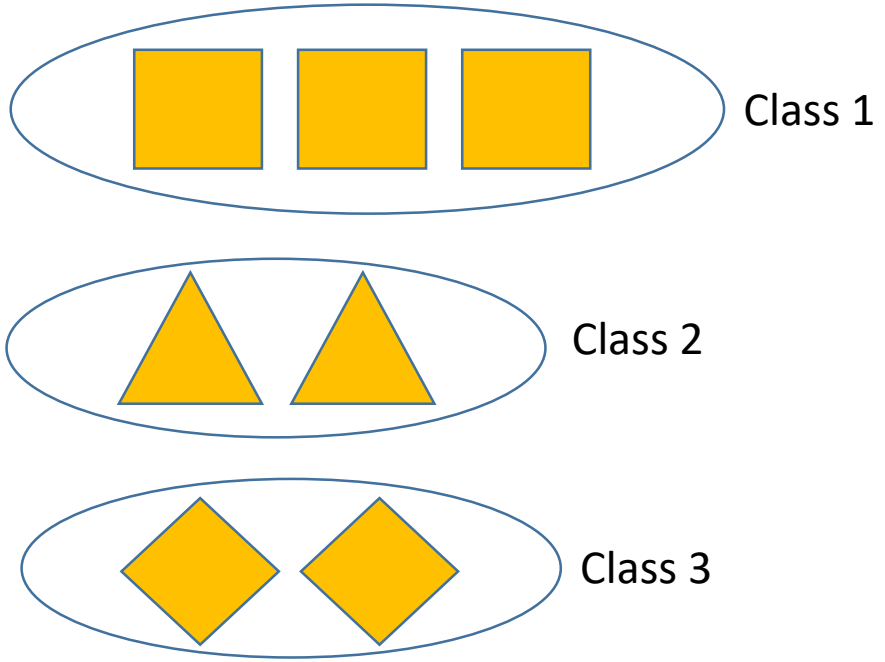


Security Landscape

Step 1. Define the interface

Step 2. Determine “(ab)normal” outputs

Step 3. List (systematically) adversary capabilities



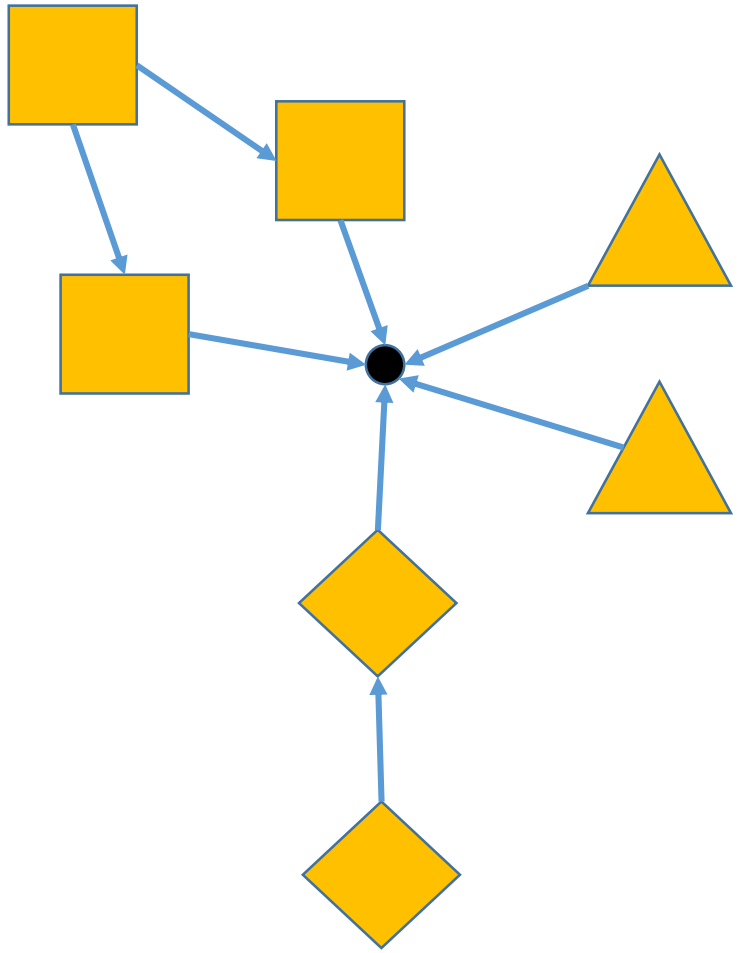
Security Landscape

Step 1. Define the interface

Step 2. Determine “(ab)normal” outputs

Step 3. List (systematically) adversary capabilities

Step 4. Identify the interdependencies of capabilities



Security Landscape

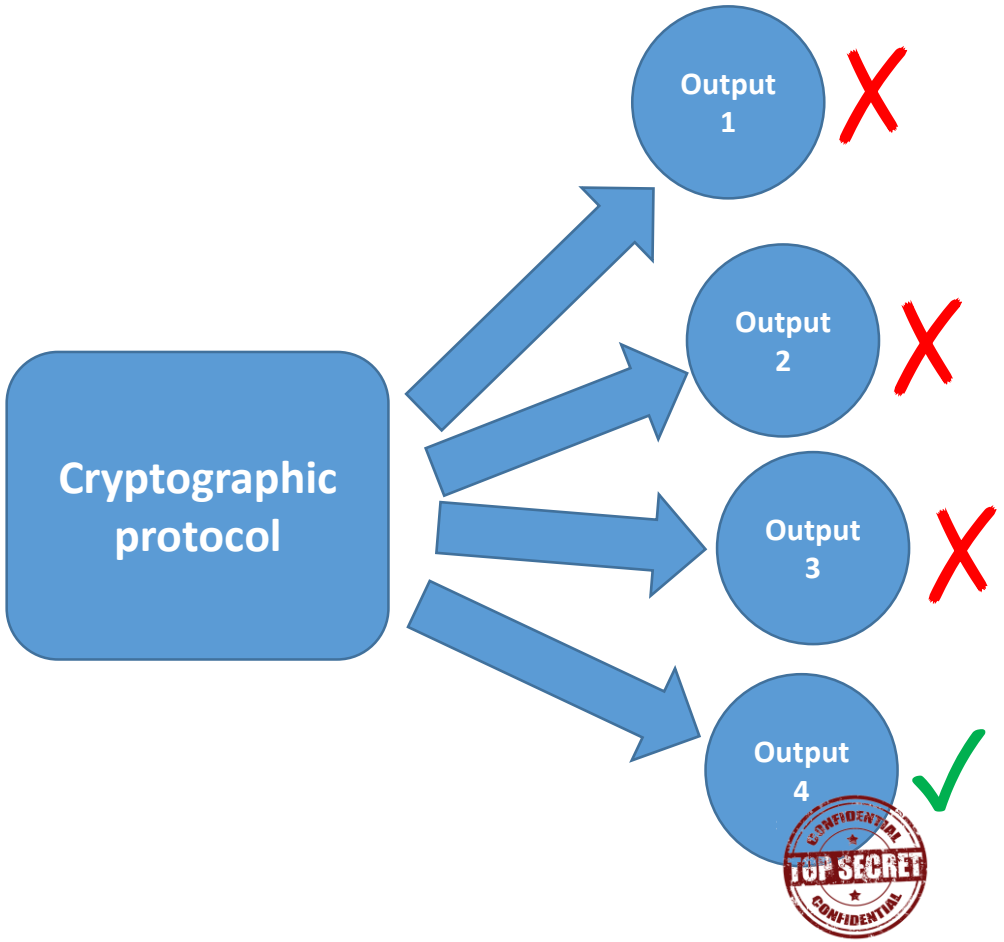
Step 1. Define the interface

Step 2. Determine “(ab)normal” outputs

Step 3. List (systematically) adversary capabilities

Step 4. Identify the interdependencies of capabilities

Step 5. List (systematically) confidential information



Security Landscape

Step 1. Define the interface

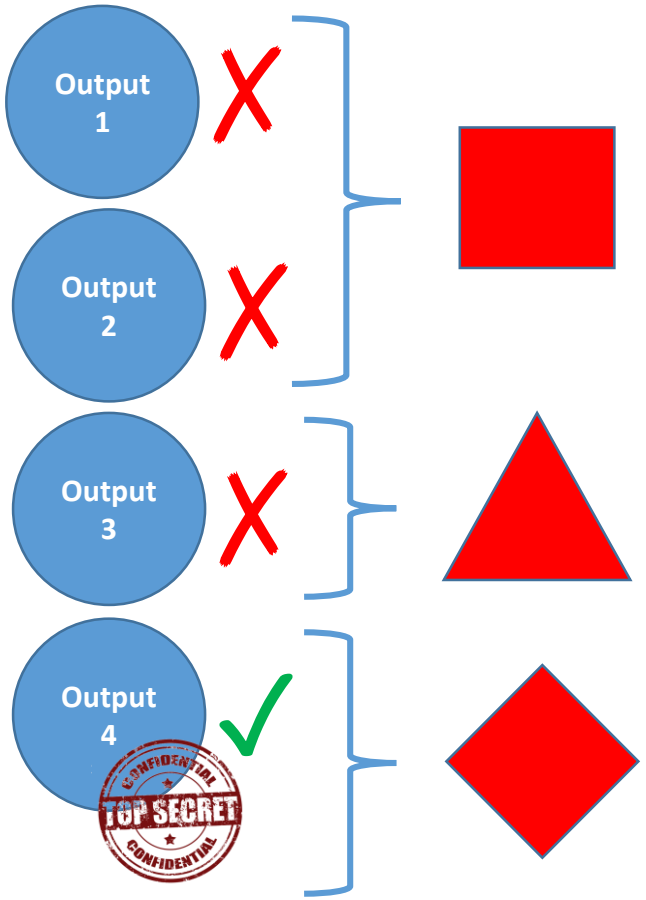
Step 2. Determine “(ab)normal” outputs

Step 3. List (systematically) adversary capabilities

Step 4. Identify the interdependencies of capabilities

Step 5. List (systematically) confidential information

Step 6. Identify threats



Security Landscape

Step 1. Define the interface

Step 2. Determine “(ab)normal” outputs

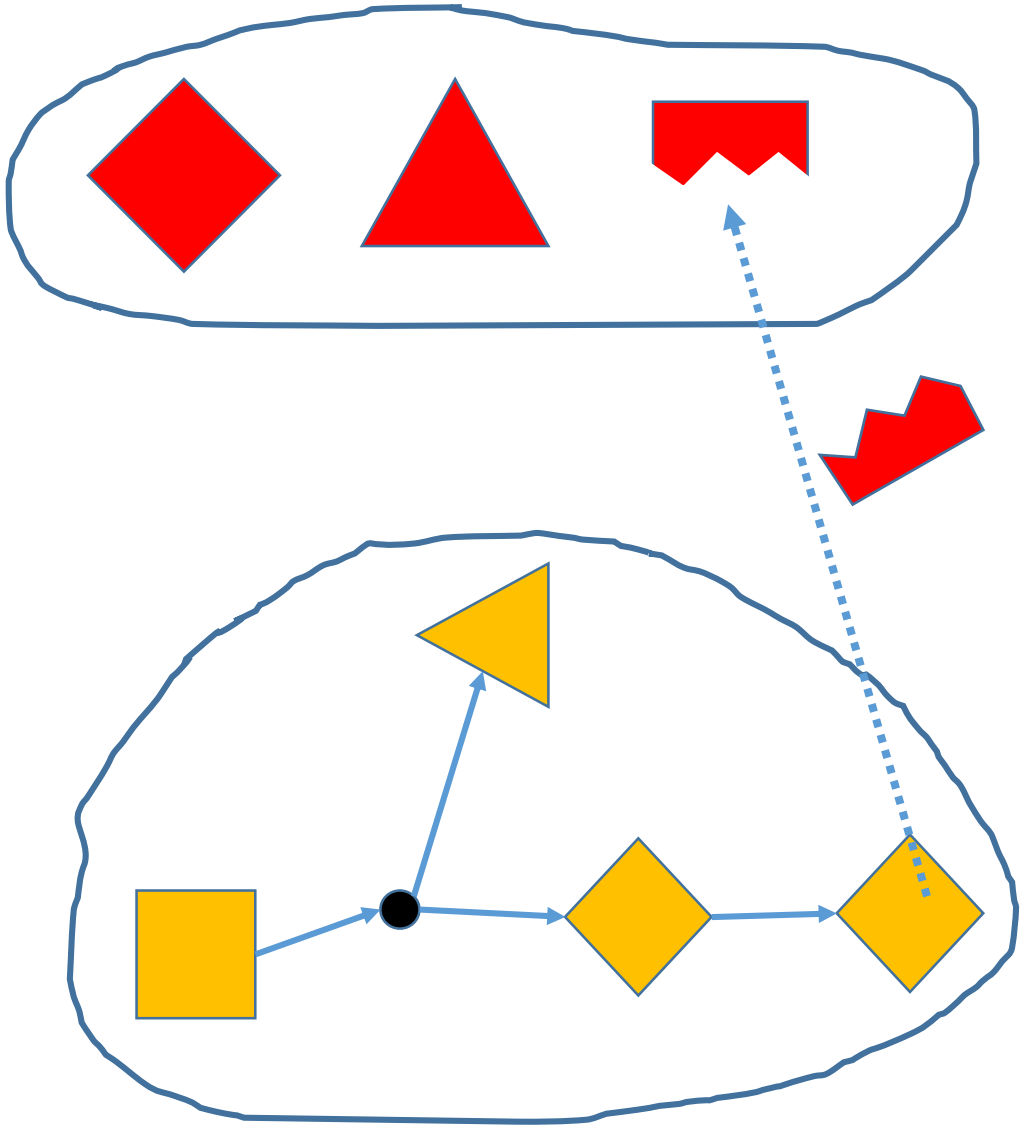
Step 3. List (systematically) adversary capabilities

Step 4. Identify the interdependencies of capabilities

Step 5. List (systematically) confidential information

Step 6. Identify threats

Step 7. Modify threats due to trivial attacks



Step 1. **Interface**

Authenticated key establishment (AKE) protocols for 2 sides

Input:
Identifiers A, B

Output of A:
S_A
K_A
R_A

Output of B:
S_B
K_B
R_B

- *with whom?* — $\{B, P_B\}$, P_B is the partner
- *what?* — established key
- *who is he?* — the role of participant

Step 1. **Interface**

Authenticated key establishment (AKE) protocols for 2 sides

Input:
Identifiers A, B

Output of A:
S_A
K_A
R_A

Output of B:
S_B
K_B
R_B

- *with whom?* — $\{B, P_B\}$, P_B is the partner
- *what?* — established key
- *who is he?* — the role of participant

Protocol outputs:
(S_A, K_A, R_A),
(S_B, K_B, R_B)

Step 2. “(Ab)normal” outputs

Output properties

$$S_A = S_B \quad K_A = K_B \quad R_A = R_B$$

$$S_A = S_B \quad K_A = K_B \quad R_A \neq R_B$$

$$S_A = S_B \quad K_A \neq K_B \quad R_A = R_B$$

$$S_A = S_B \quad K_A \neq K_B \quad R_A \neq R_B$$

$$S_A \neq S_B \quad K_A = K_B \quad R_A = R_B$$

$$S_A \neq S_B \quad K_A = K_B \quad R_A \neq R_B$$

$$S_A \neq S_B \quad K_A \neq K_B \quad R_A = R_B$$

$$S_A \neq S_B \quad K_A \neq K_B \quad R_A \neq R_B$$

Step 2. “(Ab)normal” outputs

$S_A = S_B$
$K_A = K_B$
$R_A = R_B$

$S_A = S_B$
$K_A = K_B$
$R_A \neq R_B$

$S_A = S_B$
$K_A \neq K_B$
$R_A = R_B$

$S_A = S_B$
$K_A \neq K_B$
$R_A \neq R_B$

$S_A \neq S_B$
$K_A = K_B$
$R_A = R_B$

$S_A \neq S_B$
$K_A = K_B$
$R_A \neq R_B$

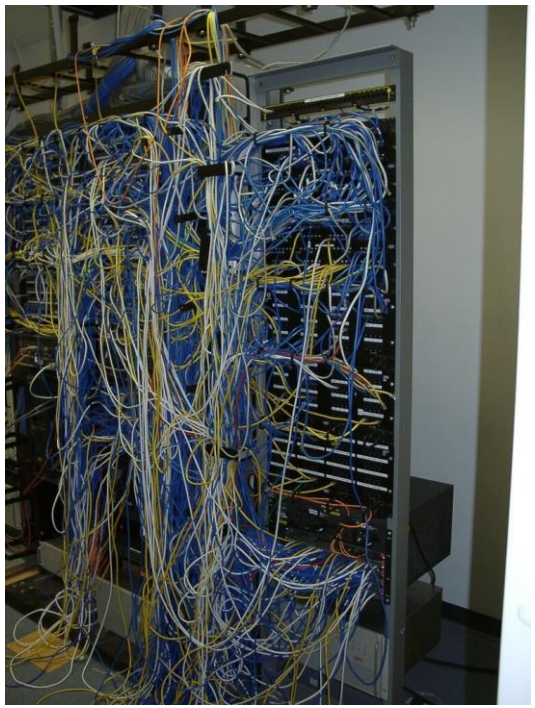
$S_A \neq S_B$
$K_A \neq K_B$
$R_A = R_B$

$S_A \neq S_B$
$K_A \neq K_B$
$R_A \neq R_B$

Step 3. **Adversary capabilities**

26 adversary capabilities from 4 classes: C, UR, AR, UA

Channel (C)



Registration of users and the adversary (UR/AR)

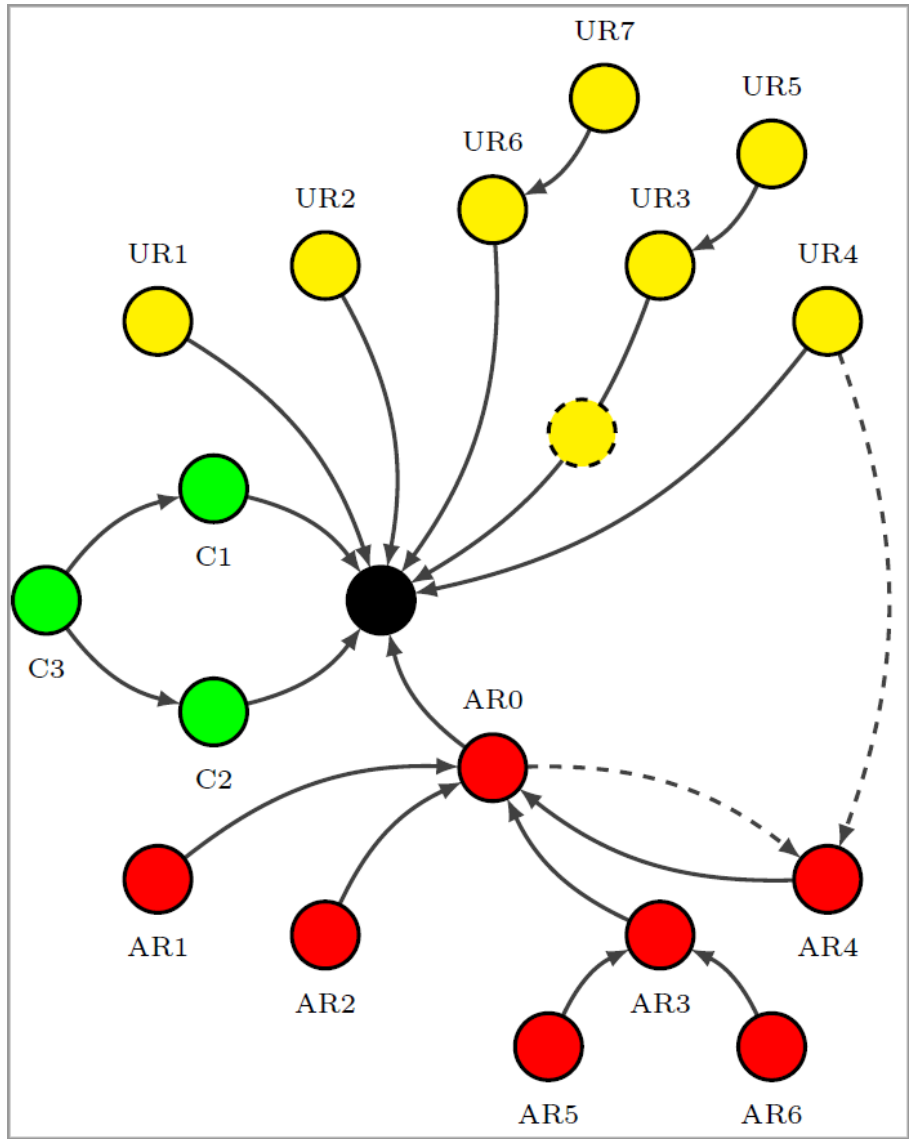
User acting after registration (UA)

Step 3. **Adversary capabilities**

Key compromise	Session key		Long-term key		Intermediate values	
	before session	after session	before session	after session	before session	after session
Secret	*no key*	✓	✓	✓	✓	✓
Public	*no public key*		✓	✓	✓	✓

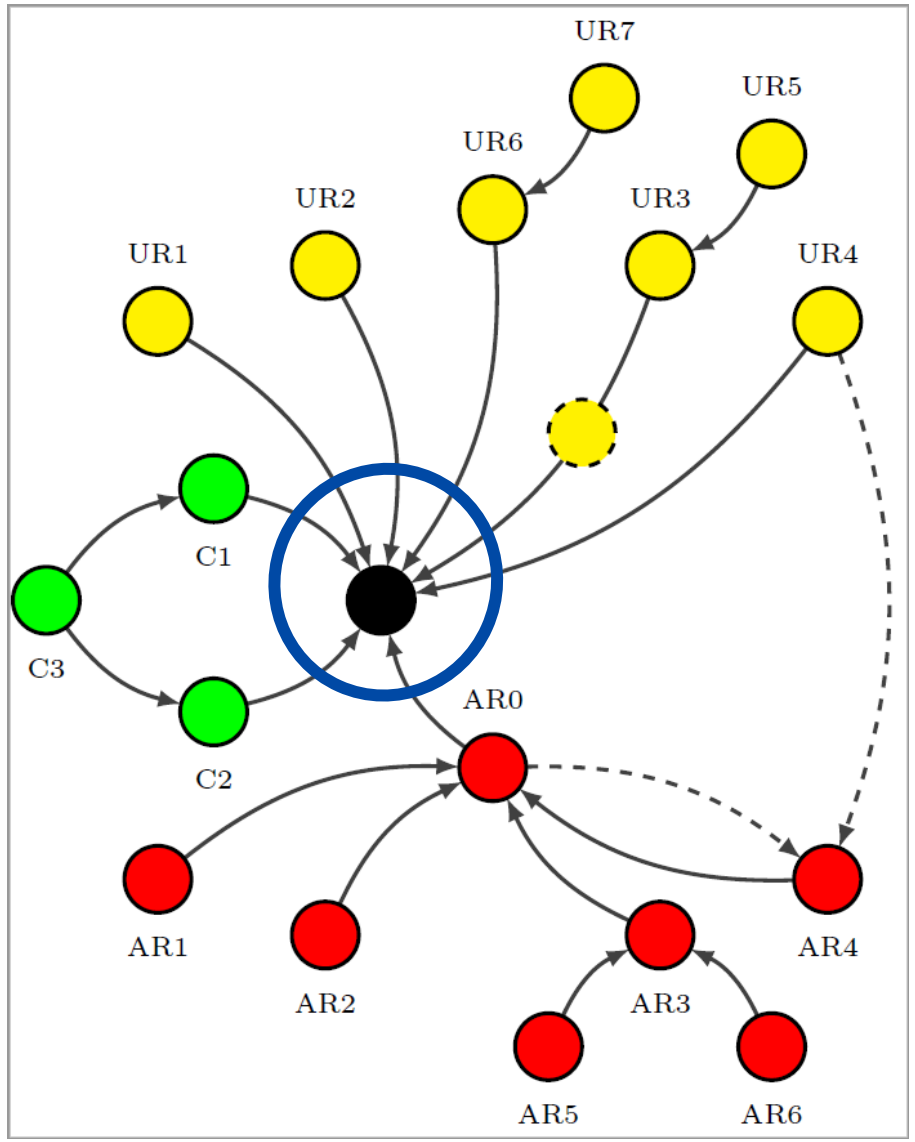
Key forcing and repeating	Long-term key		Intermediate values	
	Forcing	Repeating	Forcing	Repeating
Secret	✓	✓	✓	✓
Public	✓	*no sense*	✓	✓

Step 4. **Interdependencies of capabilities**



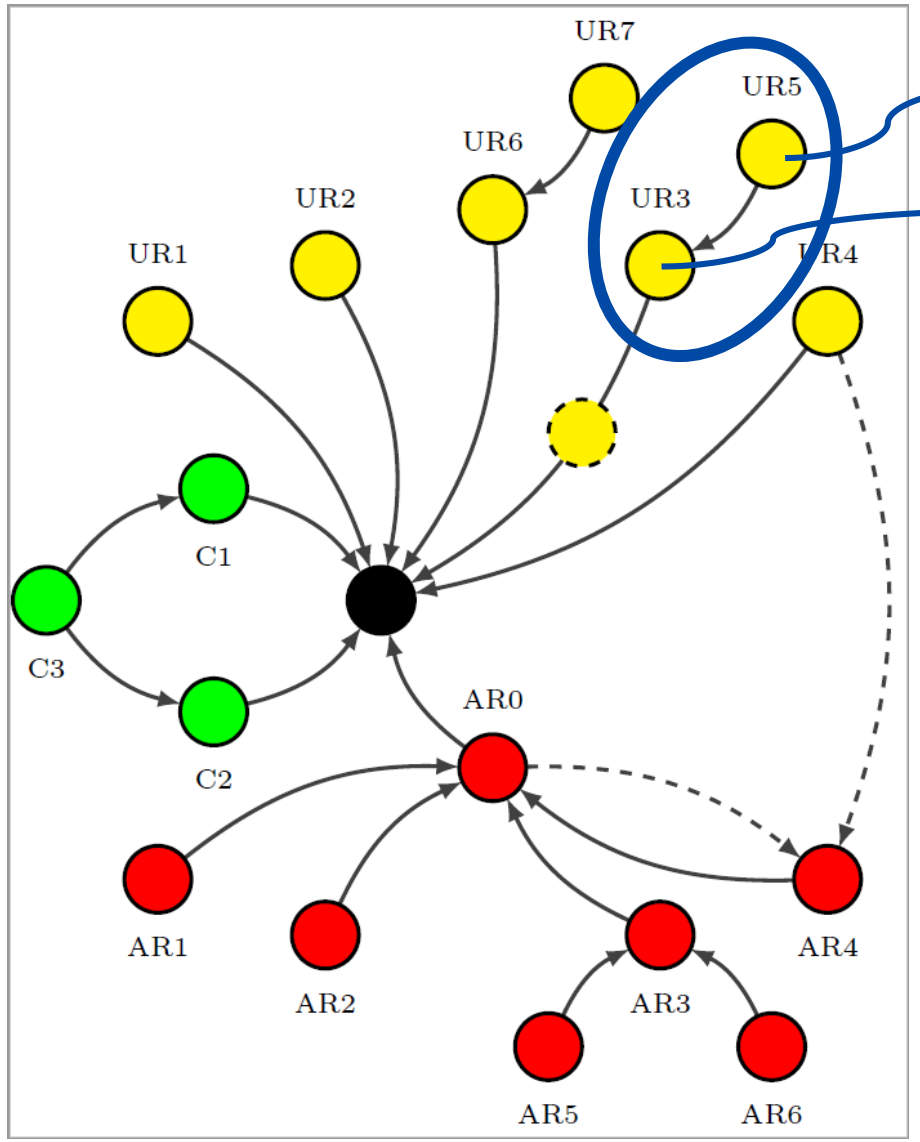
Adversary capabilities from classes C, AR, UR

Step 4. **Interdependencies of capabilities**



minimum adversary capabilities
(e.g. knowledge of public keys)

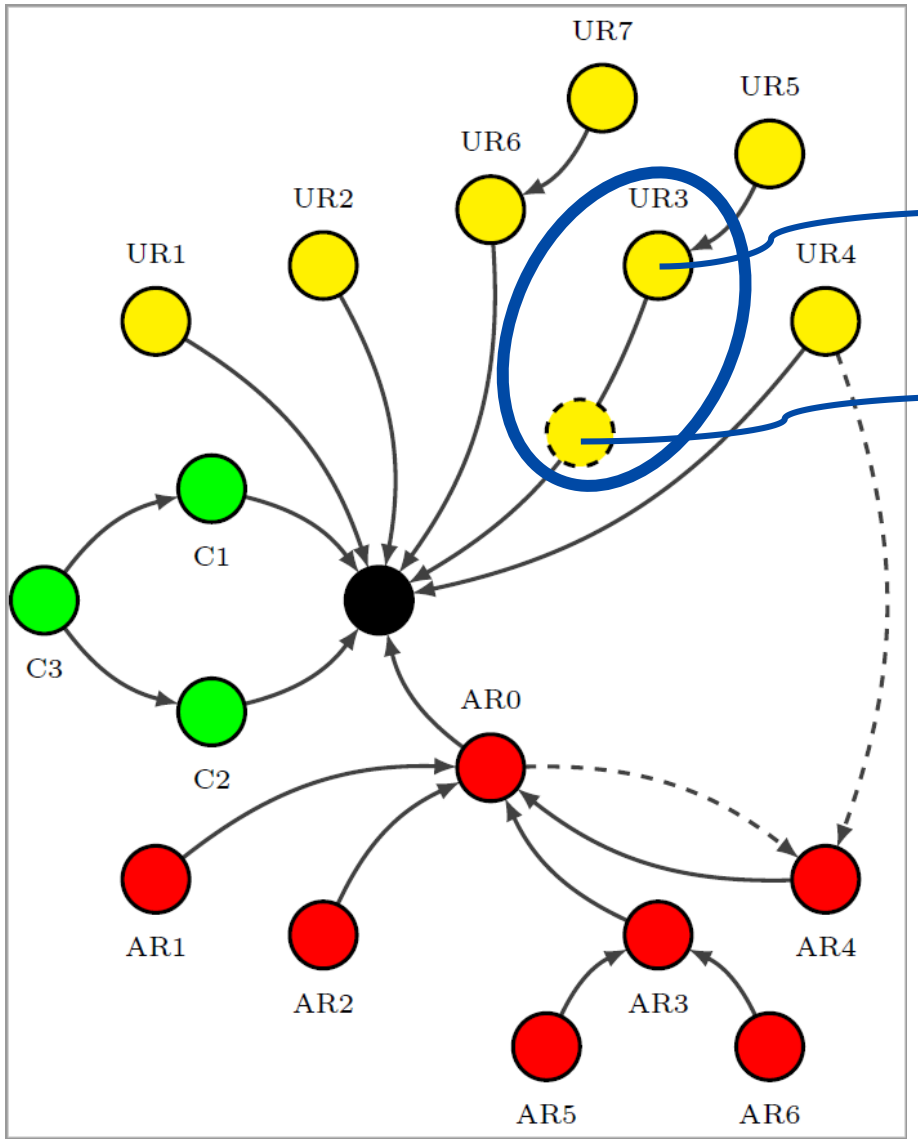
Step 4. **Interdependencies of capabilities**



Forcing inconsistent key

Forcing a key

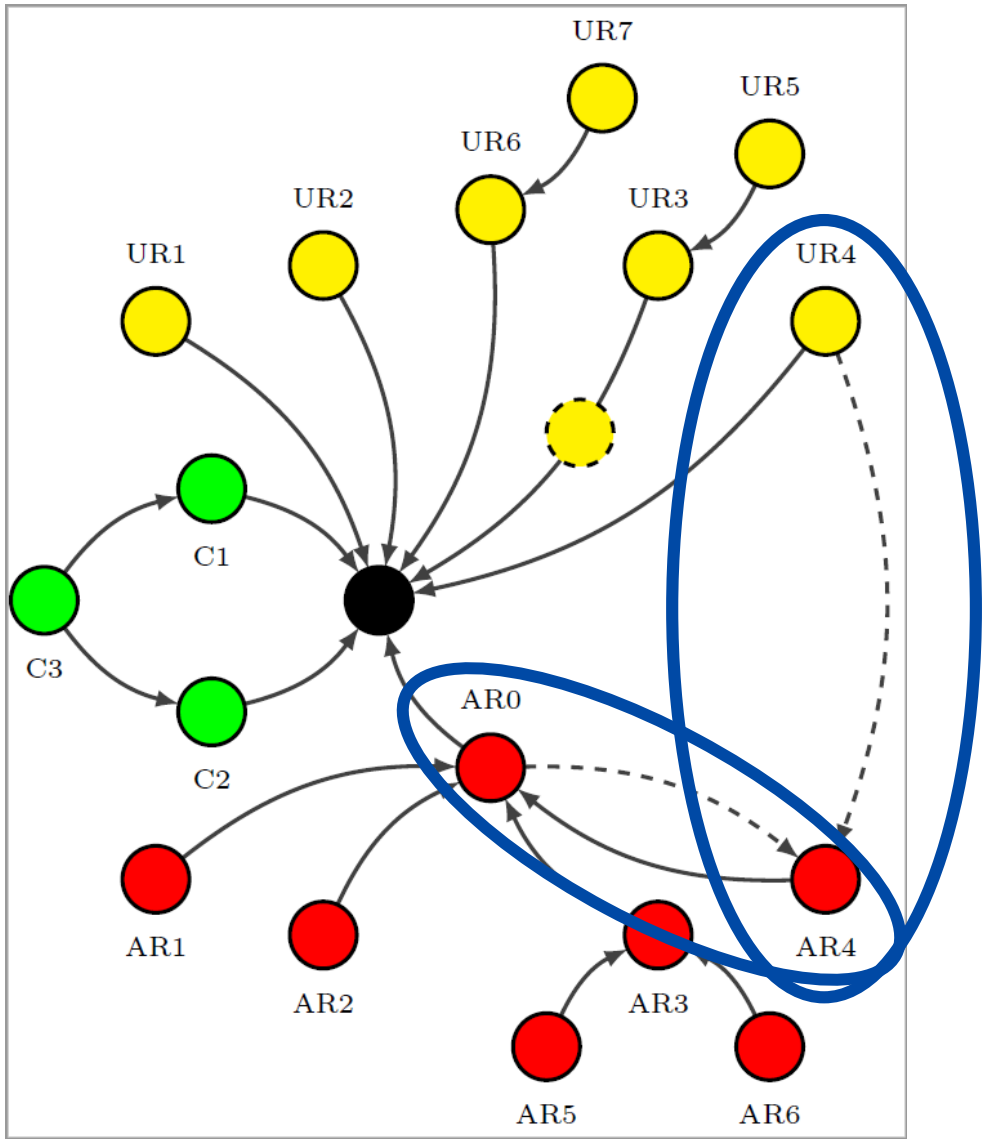
Step 4. **Interdependencies of capabilities**



Forcing a key

Forcing a key with some property

Step 4. **Interdependencies of capabilities**



the adversary has UR4 and AR0 capabilities

$\Rightarrow$ the adversary has the capability AR4

Step 5. **Confidential information**

Output of A:

S_A

K_A

R_A

Output of B:

S_B

K_B

R_B

Step 5. **Confidential information**

K_A or/and K_B are distinguishable from random for anyone other than A, B

Step 5. **Confidential information**

P_A or/and P_B are distinguishable from random for anyone other than A, B

Step 5. **Confidential information**

R_A or/and R_B are distinguishable from random for anyone other than A, B

Step 6. **Threats**

Examples of security properties **for AKE protocols** [SN22]:

- ***Message authentication*** – confirmation of the authenticity of the message source and the integrity of the transmitted message
- ***Replay protection*** – once correctly accepted by the participant, the message should not be accepted again

not the final security properties of AKE

- ***Key secrecy*** – during the interaction, the key cannot become known to the adversary, as well as to users for whom this key is not intended
- ***Key authentication*** – the participant receives confirmation that no other participant, except the second one, can know the secret key generated during the protocol execution

appear to be the same

[SN22] Nesterenko A.Yu., Semenov A.M. Methodology for assessing the security of cryptographic protocols // Prikl. Diskr. Mat. 2022. No. 56, pp. 33–82

Step 6. **Threats**

$S_A = S_B$
$K_A = K_B$
$R_A = R_B$

$S_A = S_B$
$K_A = K_B$
$R_A \neq R_B$

$S_A = S_B$
$K_A \neq K_B$
$R_A = R_B$

$S_A = S_B$
$K_A \neq K_B$
$R_A \neq R_B$

$S_A \neq S_B$
$K_A = K_B$
$R_A = R_B$

$S_A \neq S_B$
$K_A = K_B$
$R_A \neq R_B$

$S_A \neq S_B$
$K_A \neq K_B$
$R_A = R_B$

$S_A \neq S_B$
$K_A \neq K_B$
$R_A \neq R_B$

Step 6. **Threats**

$$S_A = S_B \quad K_A = K_B \quad R_A = R_B$$

$$S_A = S_B \quad K_A = K_B \quad R_A \neq R_B$$

$$S_A = S_B \quad K_A \neq K_B \quad R_A = R_B$$

$$S_A = S_B \quad K_A \neq K_B \quad R_A \neq R_B$$

$$S_A \neq S_B \quad K_A = K_B \quad R_A = R_B$$

$$S_A \neq S_B \quad K_A = K_B \quad R_A \neq R_B$$

$$S_A \neq S_B \quad K_A \neq K_B \quad R_A = R_B$$

$$S_A \neq S_B \quad K_A \neq K_B \quad R_A \neq R_B$$

Authentication Disruption

Step 6. **Threats**

Key Inequality

$S_A = S_B$
$K_A = K_B$
$R_A = R_B$

$S_A = S_B$
$K_A = K_B$
$R_A \neq R_B$

$S_A = S_B$
$K_A \neq K_B$
$R_A = R_B$

$S_A = S_B$
$K_A \neq K_B$
$R_A \neq R_B$

$S_A \neq S_B$
$K_A = K_B$
$R_A = R_B$

$S_A \neq S_B$
$K_A = K_B$
$R_A \neq R_B$

$S_A \neq S_B$
$K_A \neq K_B$
$R_A = R_B$

$S_A \neq S_B$
$K_A \neq K_B$
$R_A \neq R_B$

Authentication Disruption

Step 6. **Threats**

Key Inequality

$$S_A = S_B \quad K_A = K_B \quad R_A = R_B$$

$$S_A = S_B \quad K_A = K_B \quad R_A \neq R_B$$

$$S_A = S_B \quad K_A \neq K_B \quad R_A = R_B$$

$$S_A = S_B \quad K_A \neq K_B \quad R_A \neq R_B$$

Forcing Identical Roles (FIR) [AKS23]

$$S_A \neq S_B \quad K_A = K_B \quad R_A = R_B$$

$$S_A \neq S_B \quad K_A = K_B \quad R_A \neq R_B$$

$$S_A \neq S_B \quad K_A \neq K_B \quad R_A = R_B$$

$$S_A \neq S_B \quad K_A \neq K_B \quad R_A \neq R_B$$

Authentication Disruption

[AKS23] Alekseev E., Kyazhin S. & Smyshlyaev S. The threat of forcing the identical roles for authenticated key establishment protocols // J. Comput. Virol. Hack. Tech., 2023

Step 6. **Threats**

Authentication Disruption

$S_A \neq S_B$	$S_A \neq S_B$	$S_A \neq S_B$	$S_A \neq S_B$
$K_A = K_B$	$K_A = K_B$	$K_A \neq K_B$	$K_A \neq K_B$
$R_A = R_B$	$R_A \neq R_B$	$R_A = R_B$	$R_A \neq R_B$

Step 6. **Threats**

Authentication Disruption

$S_A \neq S_B$	$S_A \neq S_B$	$S_A \neq S_B$	$S_A \neq S_B$
$K_A = K_B$	$K_A = K_B$	$K_A \neq K_B$	$K_A \neq K_B$
$R_A = R_B$	$R_A \neq R_B$	$R_A = R_B$	$R_A \neq R_B$

Unknown Key Share (UKS)

Step 6. **Threats**

Deniability:
the output of the protocol (together with its transcript) allows the user to prove participation in the protocol session

Deniability cannot be described using our systematization ☹

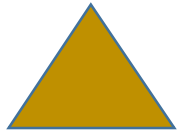
Step 7. **Threats Modification**

Impersonation resilience

Impersonate A

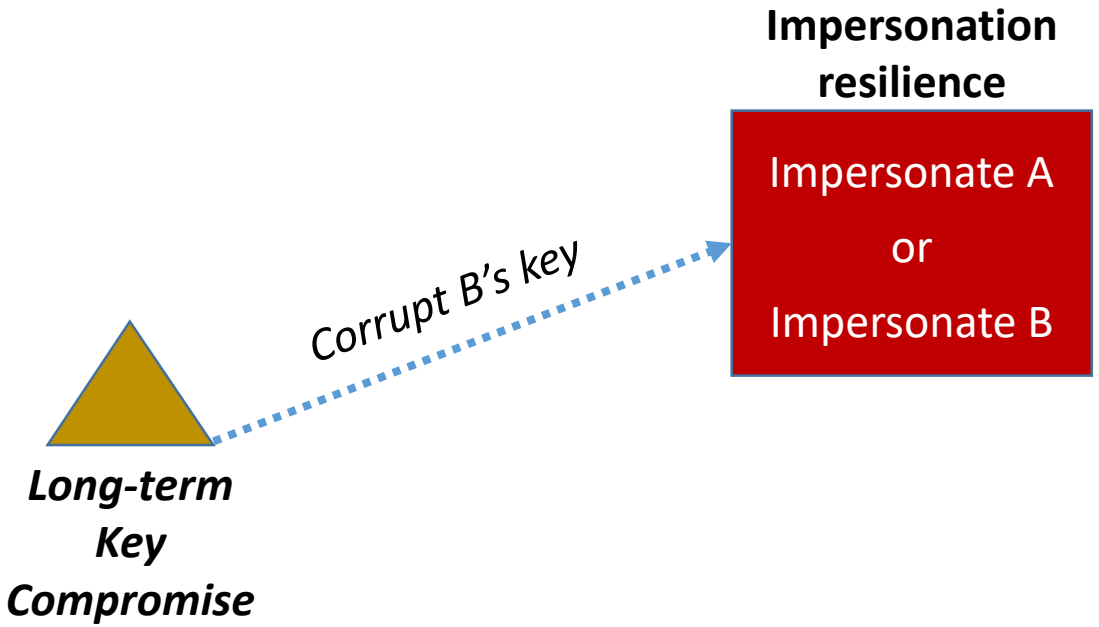
or

Impersonate B

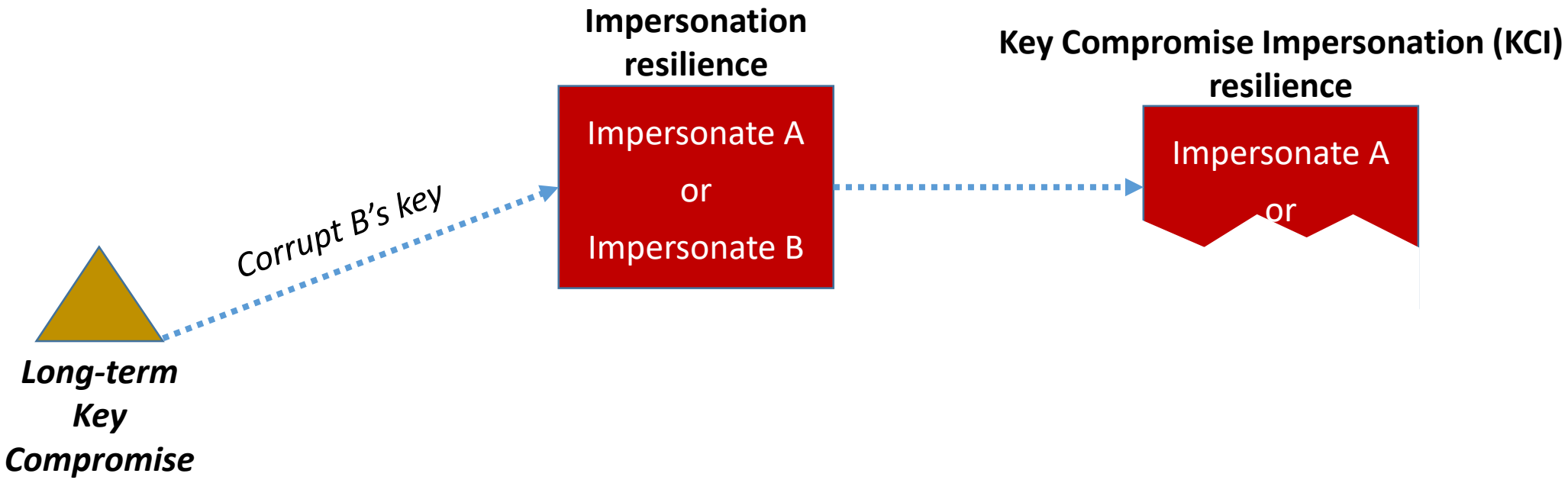


Long-term Key Compromise

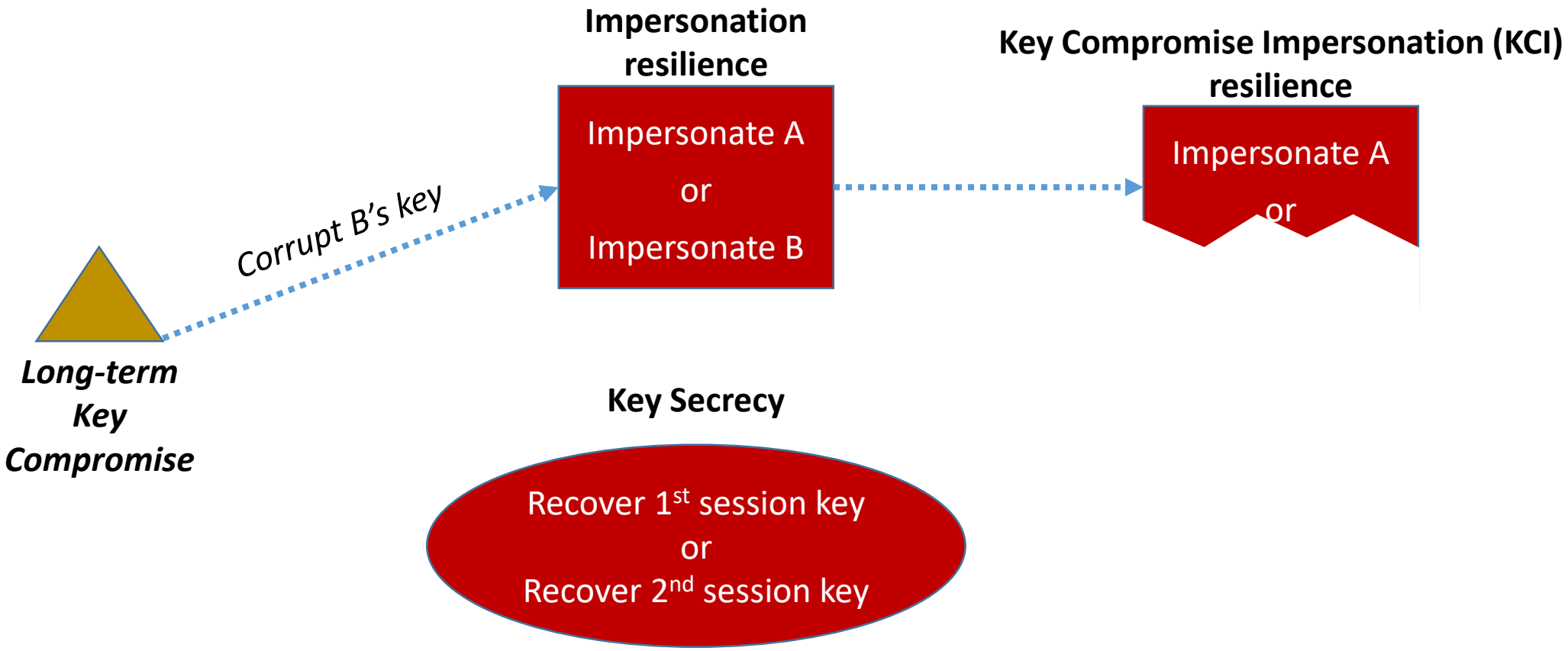
Step 7. **Threats Modification**



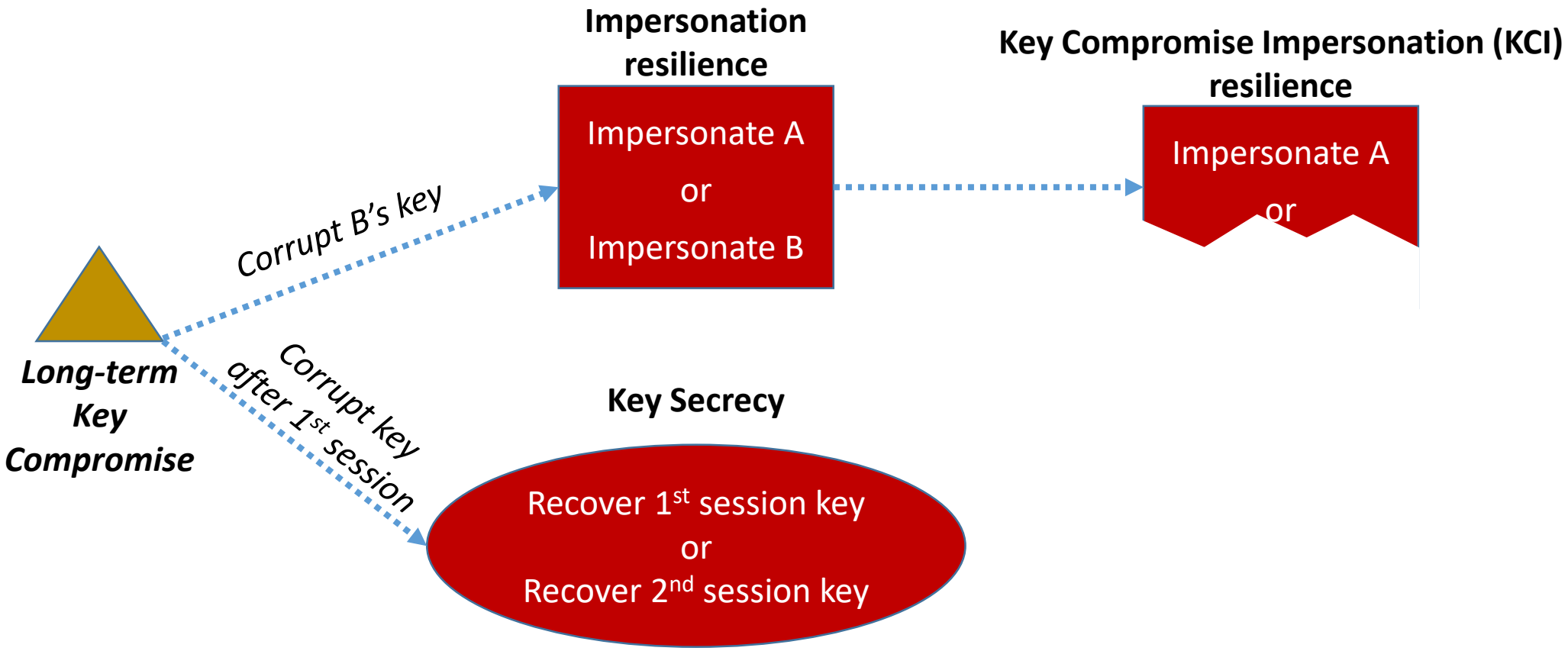
Step 7. **Threats Modification**



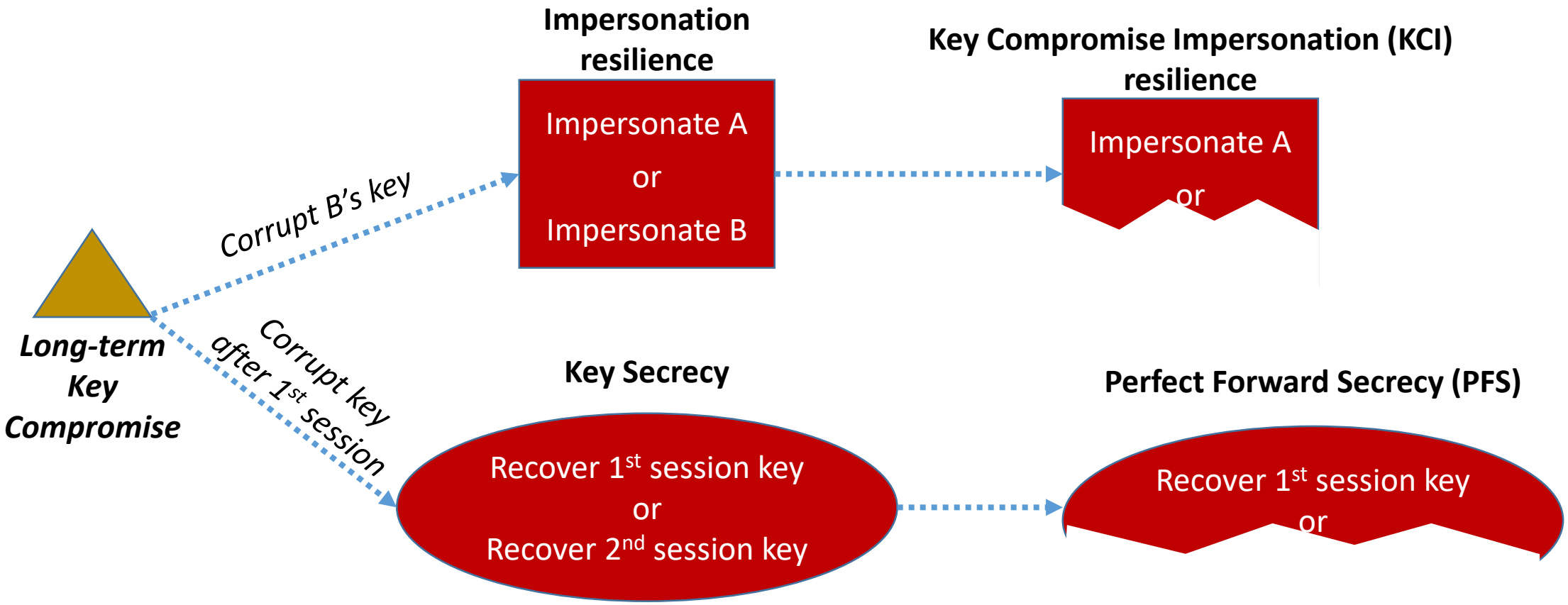
Step 7. **Threats Modification**



Step 7. **Threats Modification**



Step 7. **Threats Modification**



Additional Remarks

Seemingly independent threats can be interdependent…

Example of attack [DP18]: **KCI** $\Rightarrow$ **PFS** disruption

May be it is necessary to add Step 8. Identify the interdependencies of threats

[DP18] Dowling B., Paterson K.G. A Cryptographic Analysis of the WireGuard Protocol // Applied Cryptography and Network Security. ACNS 2018. LNCS. 2018. Vol. 10892, pp. 3–21

Interesting findings, or Conclusion

- The usual systematization of threats described in this paper is not complete (there are such security properties as deniability)
- There are subsets of AKE protocol outputs that can be considered as separate threats, but they were not previously classified as such (for example, a FIR threat)
- Seemingly independent threats can be interdependent

It is useful to form a security landscape, because otherwise something may not be taken into account (but it would be good to take everything into account)

Thank you for your attention!

kyazhin@cryptopro.ru