

On the security of one anonymous authentication protocol

A. Bakharev¹, K. Tsaregorodtsev²

1. JSRPC "Kryptonite"
2. Lomonosov Moscow State University

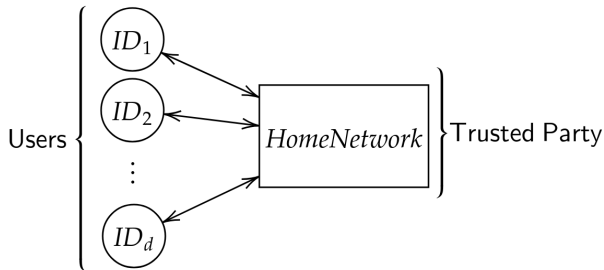
4th June 2025

Outline

- 1 Motivation and problem statement
- 2 Model
- 3 Proof Sketch
- 4 Final remarks and takeaways

A source of inspiration

- 5G-AKA protocol¹.
- Two roles: **Home Network** and **Subscriber/User**.
- The goal: to establish an authenticated session key (**AKE** protocol w/ implicit key auth.).
- A subscriber must remain anonymous from the adversarial point of view.
- Hence the security requirements: anonymity, entity authentication², session key secrecy.



¹3GPP TS 33.501 V 18.0.0. Security architecture and procedures for 5G system.

²Different from implicit/explicit key authentication

Why anonymous authentication?

- This talk: **anonymity, entity authentication**; where is the money, ~~Lebowski~~ key?
- Bottom-up analysis: start with the simple one, gradually update the model and proofs.
- In previous episodes: simple models/proofs for PRFs² and ECIES³, the security of RFID protocol⁴ (authentication), analysis of the “elementary” cryptographic mechanisms⁵.
- The final goal: security of 5G-AKA protocol⁶.

²Tsaregorodtsev, “Alternative security models for pseudorandom functions”.

³Tsaregorodtsev, “On the confidentiality and integrity of ECIES scheme”.

⁴Chichaeva et al., “On the security of one RFID authentication protocol”.

⁵Kiryukhin, “About “ k -bit security” of MACs based on hash function Streebog”, “Keyed Streebog is a secure PRF and MAC”, “Related-key attacks on the compression function of Streebog”.

⁶russian version of it

Problem statement

The object of study: interactive anonymous authentication protocol.

Cornerstones⁷: two party setting (Users, Trusted Party), pre-shared long term key.

Simplifications⁸: no inner state (counters), no key establishment, easier derivation of authentication token.

Security requirements: entity authentication, anonymity, replay/pre-play protection.

Out of scope: post-quantum security, KCI attacks, forward privacy, initial key sharing.

⁷remains untouched from 5G-AKA

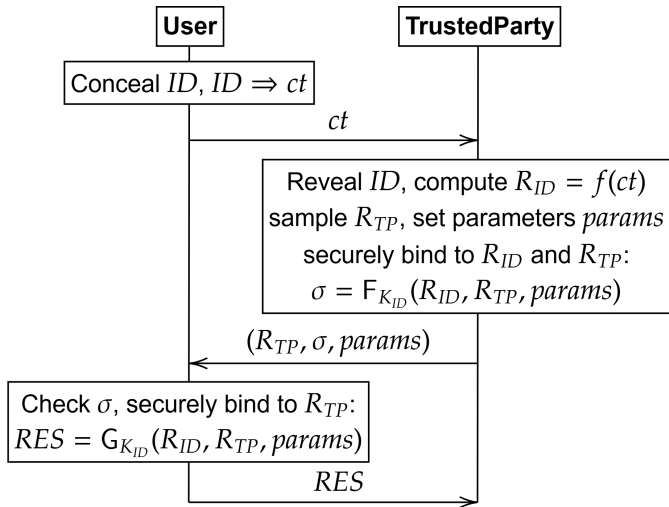
⁸even w/ all of those simplifications and previous work the model and proofs are about 50 pages long

The protocol

- Classical challenge-response structure^a.
- ID is concealed via hybrid encryption ECIES scheme^b.

^aAlferov et al., *Osnovy kriptografii* [Foundations of Cryptography].

^bAbdalla, Bellare, and Rogaway, "The oracle Diffie-Hellman assumptions and an analysis of DHIES".



Outline

- 1 Motivation and problem statement
- 2 **Model**
- 3 Proof Sketch
- 4 Final remarks and takeaways

Adversarial capabilities¹²

The adversary: computational model (time matters), an access to a set of oracles⁹ (standard “provable security” approach).

Channel: classical (Dolev-Yao) assumptions¹⁰: overhear/intercept/synthesize messages.

Registration: the adversary can choose user’s ID, no adversary registration.

After registration: parallel sessions, User-TP interaction forcing.

Out of scope: ephemeral key forcing/leakage¹¹, long-term key corruption.

⁹Katz and Lindell, *Introduction to modern cryptography*.

¹⁰Mao, *Modern Cryptography: Theory and Practice*.

¹¹Alekseev, Kyazhin, and Smyshlyaev, “Forcing future public ephemeral keys to attack authenticated key establishment protocols”.

¹²Alekseev and Kyazhin, “Probing the security landscape for authenticated key establishment protocols”.

Briefly on approaches

- Usually two types of experiments: forgery vs indistinguishability.
- **Authentication**: the probability of **forging** the session¹³.
- Alternative approach: authentication token is indistinguishable from random string¹⁴.
- **Anonymity**: two participants behave the same, i.e. **indistinguishable** from the adversarial point of view¹⁵.
- Alternative approaches: simulability¹⁶, ZK-models¹⁷.

¹³Bellare and Rogaway, “Entity authentication and key distribution”.

¹⁴Smyshlyaev et al., “On the security of one password authenticated key exchange protocol”.

¹⁵Arfaoui et al., “The privacy of the TLS 1.3 protocol”; Hermans et al., “A new RFID privacy model”; Koutsos, “The 5G-AKA Authentication Protocol Privacy”.

¹⁶Paise and Vaudenay, “Mutual authentication in RFID: security and privacy”; Vaudenay, “On privacy models for RFID”.

¹⁷Deng et al., “A zero-knowledge based framework for RFID privacy”.

What do we want?

- Unified model that for any concrete protocol Π returns single number $0 \leq \pi \leq 1$ given assumptions and model parameters.
- If π is “close to 0”, then there are no attacks in the model on protocol Π given aforementioned assumptions and parameter set.
- If π is “close to 1”, then “we are in trouble”: something bad can happen, i.e. the adversary has the strategy to attack the protocol (in the model).
- As a concrete example: IND-CCA3 model¹⁸: the adversary wins iff it is able either to forge, or to distinguish.
- General idea: a forgery task can be reformulated as an (in)distinguishability problem.

¹⁸Shrimpton, “A characterization of authenticated-encryption as a form of chosen-ciphertext security”.

The approach

Crafting the σ Auth model

1. Represent session **forgery** task as **indistinguishability** game (TestAuth^b oracle).
2. Combine it with anonymity (Draw^b oracle) in a unified model.
3. Filter out “trivial” attacks ($ID^{\text{drawn}}/ID^{\text{free}}$ sets and Match predicate).
4. Show that the model captures real-world attack scenarios (model relevance).

Oracles in the model

CreateUser(ID): create a user with a given ID (chosen by adversary),

TPSession(): start a communication session with TP,

Send(π, m): send message m to the session holder in session π ,

Result(π) : obtain session result (in-progress, accept, error, etc).

UserSession(vid): start a session with anonymised user with virtual identifier vid ,

Draw^b(ID_0, ID_1): create a virtual ID vid that is attach to one of the users (ID_0 or ID_1);
one of the adversarial goals is to “find out” which real user is bounded to vid ,

Free(vid): detach vid ,

TestAuth^b(π): if $b = 1$, then the oracle tests whether session π was successfully and non-trivially attacked by the adversary; if $b = 0$, then the oracle always returns 0.

Match predicate: filters out trivial attacks

- General idea^a: the attack is trivial if the adversary simply forwards messages $\Leftrightarrow$ session transcriptions are “almost identical” for both participants.
- In all other cases the attack is not trivial. E.g.: the adversary was able to alter some “important field” and successfully finish the protocol unnoticed, or he was able to finish authentication without any help of the second participant.

^aDowling et al., “A cryptographic analysis of the TLS 1.3 handshake protocol”.

Rand predicate: dealing with replay/pre-play attacks

- General idea: replay is possible iff there is a collision of random values, or the random value was predicted by the adversary before its generation.
- In each of these cases we give the adversary the “syntactic” opportunity to immediately win in the experiment (via query to the TestAuth^b oracle).

Estimated value

Advantage

$$\text{Adv}_{\Pi}^{\sigma\text{Auth}}(\mathcal{A}) = \Pr [\text{Exp}_{\Pi}^{\sigma\text{Auth-1}}(\mathcal{A}) \rightarrow 1] - \Pr [\text{Exp}_{\Pi}^{\sigma\text{Auth-0}}(\mathcal{A}) \rightarrow 1] .$$

InSec

$$\text{InSec}_{\Pi}^{\sigma\text{Auth}}(t, P, Q, d) = \max_{\mathcal{A} \in \mathcal{A}(t, P, Q, d)} \left(\text{Adv}_{\Pi}^{\sigma\text{Auth}}(\mathcal{A}) \right) ,$$

- maximal running time + program code $\leq t$,
- at most d Users (i.e. $\leq d$ queries to CreateUser)
- at most $P[i]$ User sessions with vid bounded to ID_i ,
- at most $Q[i]$ TP sessions with partner ID_i .

Outline

- 1 Motivation and problem statement
- 2 Model
- 3 Proof Sketch**
- 4 Final remarks and takeaways

The proof: protocol assumptions

- *ID* concealment: ECIES scheme¹⁹ is used with **VKO**²⁰ for ephemeral secret key generation and “Kuznyechik” in **CTR** and **CMAC** modes²¹ in **Encrypt-then-MAC** composition²² as AE-scheme.
- $R_{ID} = \text{Ext}(ct) = \text{Ext}(epk)$, Ext is injective.
- Keyed functions F and G used for binding are “segments” of the “Streebog-K”²³ SK:

$$F_K(x) = SK_K(x)[\ell_1 : r_1] \text{ and } G_K(x) = SK_K(x)[\ell_2 : r_2].$$

¹⁹Abdalla, Bellare, and Rogaway, “The oracle Diffie-Hellman assumptions and an analysis of DHIES”.

²⁰Alekseev et al., “On the cryptographic properties of algorithms accompanying the applications of standards GOST R 34.11-2012 and GOST R 34.10-2012”.

²¹*GOST 34.13-2018. Information technology. Cryptographic data security. Modes of operation for block ciphers.*

²²Bellare and Namprempe, “Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm”.

²³Kiryukhin, “Keyed Streebog is a secure PRF and MAC”.

The proof: main ideas, informally

- Exclude collisions/predictions of random values generated by honest participants via usual “identical-until-bad” argument $\Rightarrow$ no replay/pre-play attacks.
- Once collisions/predictions are excluded, the main model can be split into two sub-models: one for the **anonymity**, and the other for **authentication** property.
- Authentication is “secure” due to the binding to random values generated by the other party via secure pseudorandom function; reflection is also taken into consideration.
- The protocol preserves privacy due to the fact that ECIES scheme is secure in LOR-CCA model (indistinguishable encryption of different *IDs*), and segments of pseudorandom functions computed on different keys and inputs are also indistinguishable.

General view

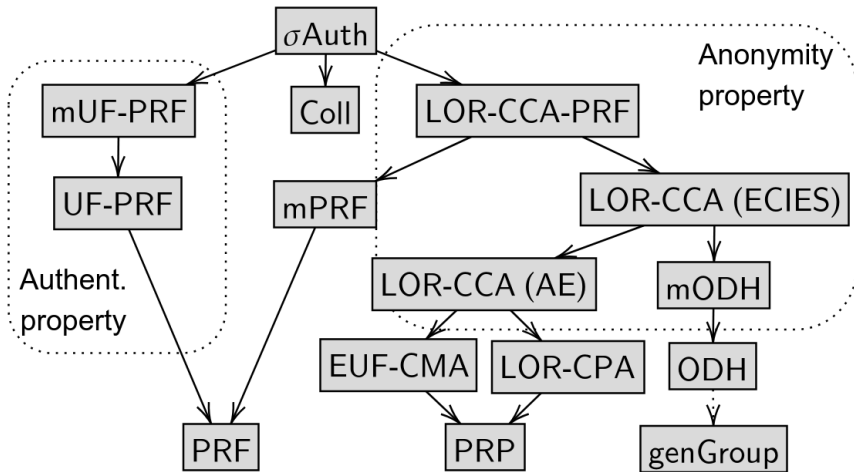
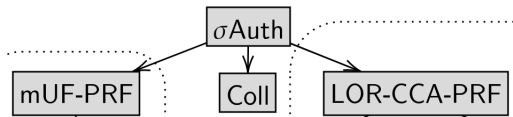


Figure: Models with m-prefix are multi-key/multi-user variants of models without prefix

Details: removing the TestAuth^b oracle

- TestAuth¹(π) returns 1
 $\Leftrightarrow$ Match = True or Rand = True.
- $\Pr[\text{Match} = \text{True}] \Leftrightarrow$
the adversary forges the segment of PRF $\Leftrightarrow$
 $\leq \text{InSec}_{\text{SK}}^{\text{mUF-PRF}}(\dots)$



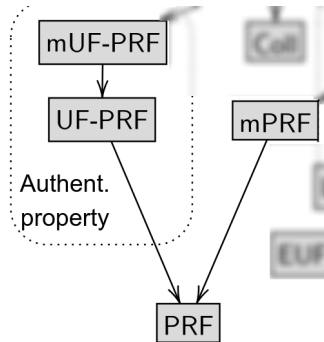
$$\Pr[\text{Rand} = \text{True}] := \Pr[\text{Coll}] \leq \frac{d \cdot p \cdot (p + q)}{2|EpkSet|} + \frac{d \cdot q \cdot (p + q)}{2^{Rlen+1}},$$

where $Rlen$ is the length of the randomness generated by TP; $EpkSet$ is a set of session public keys in $\mathbf{VKO}$; $p = \max_{1 \leq i \leq d} P[i]$, $q = \max_{1 \leq i \leq d} Q[i]$.

Details: dealing with pseudorandom functions

PRF/mPRF: distinguish the function output on any of the $d \geq 1$ keys from a random string,

UF-PRF / mUF-PRF: forge a segment of function output of $tlen$ bits in q_{vfy} tries on any of the $d \geq 1$ keys with some additional information.



$$\text{Adv}_{\text{SK}}^{\text{mPRF}}(\mathcal{A}) \leq d \cdot \text{Adv}_{\text{SK}}^{\text{PRF}}(\mathcal{B}), \quad \text{Adv}_{\text{SK}}^{\text{mUF-PRF}}(\mathcal{A}) \leq d \cdot \text{Adv}_{\text{SK}}^{\text{UF-PRF}}(\mathcal{B}),$$

$$\text{Adv}_{\text{SK}}^{\text{UF-PRF}}(\mathcal{A}) \leq \text{Adv}_{\text{SK}}^{\text{PRF}}(\mathcal{B}) + \frac{q_{vfy}}{2^{tlen}}.$$

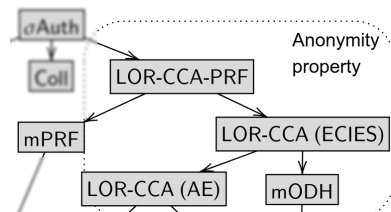
Details: dealing with ECIES scheme

mODH: distinguish keys generated by KE from random.

LOR-CCA/mLOR-CCA: distinguish which one of the messages (left/right) has been encrypted

LOR-CCA for ECIES: the extension of classical model, secret keys are generated by KE and used in AE.

LOR-CCA-PRF: combination of mPRF & LOR-CCA for ECIES scheme.



$$\text{Adv}_{\text{AE}}^{\text{mLOR-CCA}}(\mathcal{A}) \leq d \cdot \text{Adv}_{\text{AE}}^{\text{LOR-CCA}}(\mathcal{B}), \quad \text{Adv}_{\text{SK,ECIES}}^{\text{LOR-CCA-PRF}}(\mathcal{A}) \leq \text{Adv}_{\text{SK}}^{\text{mPRF}}(\mathcal{B}) + \text{Adv}_{\text{ECIES}}^{\text{LOR-CCA}}(\mathcal{C})$$

$$\text{Adv}_{\text{ECIES}}^{\text{LOR-CCA}}(\mathcal{A}) \leq \text{Adv}_{\text{AE}}^{\text{mLOR-CCA}}(\mathcal{B}) + \text{Adv}_{\text{KE}}^{\text{mODH}}(\mathcal{C}) + \dots$$

Intermediate results

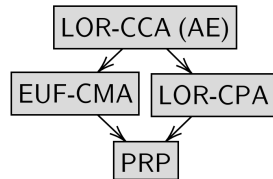
$$\begin{aligned} \text{InSec}_{\Pi}^{\sigma\text{Auth}}(t, P, Q, d) &\leq dp \cdot \text{InSec}_{\text{AE}}^{\text{LOR-CCA}}(t + T, 1, \mu, dq, \mu) + 2 \cdot \text{InSec}_{\text{KE}}^{\text{mODH}}(t + T, dp, dq) \\ &\quad + 2d \cdot \text{InSec}_{\text{SK}}^{\text{PRF}}(t + T, 2p + q) + 4d \cdot \text{InSec}_{\text{SK}}^{\text{PRF}}(t + T, 3p + 3q) \\ &\quad + \frac{d^2 p(p + 2q)}{|EpkSet|} + \frac{d(p + q)}{2^{tlen-1}} + \frac{dp(p + q)}{2|EpkSet|} + \frac{dq(p + q)}{2^{Rlen+1}}, \end{aligned}$$

where the following notation is used: μ is the length of the ID (in blocks),

$$p = \max_{1 \leq i \leq d} P[i], \quad q = \max_{1 \leq i \leq d} Q[i], \quad T = 18d \cdot (p + q + 1).$$

Subproblem analysis I

- Keyed hash function «Streebog-K» SK in PRF model²⁴
- AE = **CTR** + **CMAC** on independent keys, **Encrypt-then-MAC** composition²⁵, Kuznyechik block cipher



$$\begin{aligned} \text{InSec}_{\text{SK}}^{\text{PRF}}(t, q) &\leq \frac{t}{2^{256}} + \frac{3 \cdot t \cdot q + 1.5 \cdot (q^2 + 2q)}{2^{512}}, & \text{InSec}_{\text{AE}}^{\text{LOR-CCA}}(t, q_e, \mu_e, q_d, \mu_d) &\leq \\ &\leq \frac{40 q_d (q_e + q_d)^2 + 46 q_d (q_e + q_d) \mu^2 + 2(q_e \mu_e)^2 + 2q_d}{2^{128}} + \frac{t + (q_e + q_d) \mu}{2^{254}}. \end{aligned}$$

²⁴Kiryukhin, “About “ k -bit security” of MACs based on hash function Streebog”.

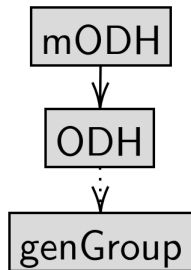
²⁵Chattopadhyay, Jha, and Nandi, “Towards tight security bounds for OMAC, XCBC and TMAC”.

Subproblem analysis II

- $\text{KE} = \text{VKO}$ scheme with fixed UKM , hash function in VKO is modeled as a random oracle ²⁶,
- only universal DLOG algorithms (generic group model ²⁷) are considered.

$$\text{InSec}_{\text{VKO}}^{\text{mODH}}(t, q_{\text{gen}}, q_{\text{com}}) \leq q_{\text{gen}} \cdot \frac{2 \cdot (q_{\text{group}} + q_{\text{com}})^2}{|EpkSet|} + \frac{2 q_{\text{gen}} q_{\text{com}}}{|EpkSet|},$$

q_{group} is the number of queries to the generic group oracle ²⁸.



²⁸Bellare and Rogaway, “Random oracles are practical: A paradigm for designing efficient protocols”.

²⁸Nechaev, “Complexity of a determinate algorithm for the discrete logarithm”; Shoup, “Lower bounds for discrete logarithms and related problems”.

²⁸Bakharev and Tsaregorodtsev, “On the security of some algorithms over a group of points of elliptic curves”; Tsaregorodtsev, “On the confidentiality and integrity of ECIES scheme”.

Outline

- 1 Motivation and problem statement
- 2 Model
- 3 Proof Sketch
- 4 Final remarks and takeaways

Some takeaways

- The anonymous authentication protocol based on 5G-AKA key agreement procedure was presented; the protocol follows the main steps of 5G-AKA with some simplifications.
- The protocol was analyzed in the dedicated security model σAuth which captures authentication and privacy properties, as well as some real-world attack scenarios.
- We see the work as a significant stepping stone to the final destination point (the security of 5G-AKA protocol): main building blocks are presented, two out of three main security properties are captured, the interactivity is taken into account.
- **Counter/inner state handling:** they DO hurt, but not so much — due to the fact that parties bind to random values that do not collide.

What else can be done: model and adversary

- Generalize the model: include session key generation and its indistinguishability from completely random values²⁹; roles and ephemeral key leakage/forcing³⁰.
- Add participant inner state and show the security of full 5G-AKA-GOST protocol.
- Weaken the adversary: one forgery is not enough³¹.
- Remove technical obstacles, i.e., consider non-injective Ext function.
- Weaken idealized assumptions (ROM, generic group model).

²⁹Boyd, Mathuria, and Stebila, *Protocols for authentication and key establishment*; Dowling et al., “A cryptographic analysis of the TLS 1.3 handshake protocol”.

³⁰Alekseev and Kyazhin, “Probing the security landscape for authenticated key establishment protocols”; Alekseev, Kyazhin, and Smyshlyaev, “The threat of forcing the identical roles for authenticated key establishment protocols”; Alekseev, Kyazhin, and Smyshlyaev, “Forcing future public ephemeral keys to attack authenticated key establishment protocols”.

³¹Kiryukhin, “On the one method of key lifetime estimation for CRISP and IPLir protocols”.

Thank you for your attention!

Our **sincere gratitude** to all the anonymous reviewers

Bibliography I

-  3GPP TS 33.501 V 18.0.0. *Security architecture and procedures for 5G system.*
-  Abdalla, M., M. Bellare, and P. Rogaway. “The oracle Diffie-Hellman assumptions and an analysis of DHIES”. In: *CT-RSA 2001*. Springer. 2001, pp. 143–158.
-  Alekseev, E. and S. Kyazhin. “Probing the security landscape for authenticated key establishment protocols”. In: *The 12th Workshop on Current Trends in Cryptology (CTCrypt 2023)*. 2023.
-  Alekseev, E., S. Kyazhin, and S. Smyshlyaev. “Forcing future public ephemeral keys to attack authenticated key establishment protocols”. In: *Prikladnaya diskretnaya matematika* 66 (2024), pp. 60–77.
-  — . “The threat of forcing the identical roles for authenticated key establishment protocols”. In: *Journal of Computer Virology and Hacking Techniques* 20.2 (2024), pp. 225–230.

Bibliography II

-  Alekseev, E. K., S. N. Kyazhin, and S. V. Smyshlyaev. “Forcing future public ephemeral keys to attack authenticated key establishment protocols”. In: *Prikladnaya Diskretnaya Matematika* 66 (2024), pp. 60–77.
-  Alekseev, E. K. et al. “On the cryptographic properties of algorithms accompanying the applications of standards GOST R 34.11-2012 and GOST R 34.10-2012”. In: *Mathematical Aspects of Cryptography* 7.1 (2016), pp. 5–38.
-  Alferov, A. P. et al. *Osnovy kriptografii [Foundations of Cryptography]*. In Russian. Moscow: Helios, Association of Russian Universities, 2005, p. 480.
-  Arfaoui, G. et al. “The privacy of the TLS 1.3 protocol”. In: *Proceedings on Privacy Enhancing Technologies* (2019), pp. 190–210.
-  Bakharev, A. and K. Tsaregorodtsev. “On the security of some algorithms over a group of points of elliptic curves”. In: *Applied Discrete Mathematics. Supplement* 17 (2024), pp. 63–70.

Bibliography III

-  Bellare, B. and C. Namprempre. “Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm”. In: *Journal of Cryptology* 21 (2000), pp. 469–491.
-  Bellare, M. and P. Rogaway. “Entity authentication and key distribution”. In: *Annual international cryptology conference*. Springer. 1993, pp. 232–249.
-  —. “Random oracles are practical: A paradigm for designing efficient protocols”. In: (1993), pp. 62–73.
-  Boyd, C., A. Mathuria, and D. Stebila. *Protocols for authentication and key establishment*. Springer, 2003.
-  Chattopadhyay, S., A. Jha, and M. Nandi. “Towards tight security bounds for OMAC, XCBC and TMAC”. In: (2023), pp. 348–378.
-  Chichaeva, A. et al. “On the security of one RFID authentication protocol”. In: *Mathematical Aspects of Cryptography* 16.1 (2025). (In russian), pp. 29–84.

Bibliography IV

-  Deng, R. H. et al. “A zero-knowledge based framework for RFID privacy”. In: *Journal of Computer Security* 19.6 (2011), pp. 1109–1146.
-  Dowling, B. et al. “A cryptographic analysis of the TLS 1.3 handshake protocol”. In: *Journal of Cryptology* 34.4 (2021), pp. 1–69.
-  GOST 34.13-2018. *Information technology. Cryptographic data security. Modes of operation for block ciphers*. Russian. 2018.
-  Hermans, J. et al. “A new RFID privacy model”. In: *European symposium on research in computer security*. Springer. 2011, pp. 568–587.
-  Katz, J. and Y. Lindell. *Introduction to modern cryptography*. CRC press, 2020.
-  Kiryukhin, Vitalii Aleksandrovich. “About “ k -bit security” of MACs based on hash function Streebog”. In: *Mathematical Aspects of Cryptography* 15.2 (2024). (In russian), pp. 47–68.

Bibliography V

-  Kiryukhin, Vitalii Aleksandrovich. “Keyed Streebog is a secure PRF and MAC”. In: *Mathematical Aspects of Cryptography* 14.2 (2023), pp. 77–96.
-  — . “On the one method of key lifetime estimation for CRISP and IPLir protocols”. In: *RusCrypto’25*. (In russian). 2025.
-  — . “Related-key attacks on the compression function of Streebog”. In: *Mathematical Aspects of Cryptography* 14.2 (2023), pp. 59–76.
-  Koutsos, A. “The 5G-AKA Authentication Protocol Privacy”. In: June 2019, pp. 464–479. DOI: 10.1109/EuroSP.2019.00041.
-  Mao, W. *Modern Cryptography: Theory and Practice*. In Russian. Williams publishing, 2005.
-  Nechaev, V. “Complexity of a determinate algorithm for the discrete logarithm”. In: *Math. Notes* 55.2 (1994), pp. 91–101.

Bibliography VI

-  Paise, R. I. and S. Vaudenay. “Mutual authentication in RFID: security and privacy”. In: *Proceedings of the 2008 ACM symposium on Information, computer and communications security*. 2008, pp. 292–299.
-  Shoup, V. “Lower bounds for discrete logarithms and related problems”. In: *EURO-CRYPT’97*. Springer, 1997, pp. 256–266.
-  Shrimpton, Tom. “A characterization of authenticated-encryption as a form of chosen-ciphertext security”. In: *Cryptology ePrint Archive* (2004).
-  Smyshlyaev, S. V. et al. “On the security of one password authenticated key exchange protocol”. In: *Cryptology ePrint Archive* (2015).
-  Tsaregorodtsev, K. “Alternative security models for pseudorandom functions”. In: *Mathematical Aspects of Cryptography* 15.3 (2024). (In russian), pp. 113–134.
-  —. “On the confidentiality and integrity of ECIES scheme”. In: *Mathematical Aspects of Cryptography* 15.2 (2024). (In russian), pp. 101–136.



Vaudenay, S. “On privacy models for RFID”. In: *International conference on the theory and application of cryptology and information security*. Springer. 2007, pp. 68–87.