APPENDIX

A. Proofs of Section IV

In the following, we assume that Σ consists of a set of disjunctive s-t GAV mappings.

First, by adapting the proof of Theorem 16 from [3], we can show that the following holds

Proposition A.3. *A mapping $\mathscr{M} = (\mathsf{S}, \mathsf{T}, \Sigma)$ does not disclose a constant-free CQ p over S on any instance of S, iff $\vec{*} \notin p(J)$, where $J = I_{\mathsf{S}}(\Sigma_{st})$.* □

Proposition A.3 states that, in order to check if a constant-free CQ is safe according to Definition 2, we need to check if the critical tuple is among the answers to p over the instance computed by $\mathsf{visChase}_{\mathsf{S}}(\Sigma)$.

We are now ready to prove Theorem 1.

Theorem 1. *A mapping $\mathscr{M}_2 = (\mathsf{S}, \mathsf{T}_2, \Sigma_2)$ preserves the privacy of a mapping $\mathscr{M}_1 = (\mathsf{S}, \mathsf{T}_1, \Sigma_1)$ on all instances of S, if and only if there exists a homomorphism from $I_{\mathsf{S}}(\Sigma_2)$ into $I_{\mathsf{S}}(\Sigma_1)$ that preserves the critical constant $*$.* □

Proof. The proof of Theorem 1 depends upon the following lemma.

Lemma 1. *Given two instances I_1 and I_2, the following are equivalent*

1) *for every conjunctive query p, if $\vec{u} \in p(I_1)$, then $\vec{u} \in p(I_2)$, where $\vec{u}$ is a vector of constants*
2) *there exists a homomorphism from I_1 to I_2 preserving the constants of I_1*

Proof of Lemma 1. (2)⇒(1). Suppose that there exists a homomorphism h from I_1 to I_2 preserving the constants of I_1. Suppose also that $\vec{u} \in p(I_1)$, with p being a conjunctive query. This means that there exists a homomorphism h_1 from p into I_1 mapping each free variable x_i of p into u_i, for each $1 \leq i \leq n$, where n is the number of free variables of p. Since the composition of two homomorphisms is a homomorphism and since h preserves the constants of I_1 due to the base assumptions, this means that $h \circ h_1$ is a homomorphism from p into I_2 mapping each free variable x_i of p into t_i, for each $1 \leq i \leq n$. This completes this part of the proof.

(1)⇒(2). Let p_1 be a conjunctive query formed by creating a non-ground atom $R(y_1, \ldots, y_n)$ for each ground atom $R(u_1, \ldots, u_n) \in I_1$, by taking the conjunction of these non-ground atoms and by converting into an existentially quantified variable every variable created out of some labelled null. Let $\vec{x}$ denote the free variables of p_1 and let $n = |\vec{x}|$. From the above, it follows that there exists a homomorphism h_1 from p_1 into I_1 mapping each $x_i \in \vec{x}$ into some constant occurring in I_1. Let $\vec{u} \in p_1(I_1)$. From (1), it follows that $\vec{u} \in p_1(I_2)$ and, hence, there exists a homomorphism h_2 from p_1 into I_2 mapping each $x_i \in \vec{x}$ into u_i, for each $1 \leq i \leq n$. Since h_1 ranges over all constants of I_1 and since $h_1(x_i) = h_2(x_i)$ holds for each $1 \leq i \leq n$, it follows that there exists a homomorphism from I_1 to I_2 preserving the constants of I_1. This completes the second part of the proof. □

Lemma 1 can be restated as follows

Lemma 2. *Given two instances I_1 and I_2, the following are equivalent*

1) *for every conjunctive query p, if $\vec{t} \notin p(I_2)$, then $\vec{t} \notin p(I_1)$*
2) *there exists a homomorphism from I_1 to I_2*

We are now ready to return to the main part of the proof.

Given a query p over a source schema S, and a mapping $\mathscr{M}$ defined as the triple $(\mathsf{S}, \mathsf{T}, \Sigma)$, where T is a target schema and Σ is a set of s-t dependencies, we know from Proposition A.3 that if $\mathscr{M}$ discloses p on some instance of S, then there exists a homomorphism of p into $\mathsf{visChase}_{\mathsf{S}}(\Sigma)$ mapping the free variables of p into the critical constant $*$.

From the above, we know that $\mathscr{M}_2$ does not preserve the privacy of $\mathscr{M}_1$ if there exists a query p over S, such that $\vec{*} \notin J_1$ and $\vec{*} \in J_2$, where $J_1 = I_{\mathsf{S}}(\Sigma_1)$ and $J_2 = I_{\mathsf{S}}(\Sigma_2)$. We will now prove that $\mathscr{M}_2$ preserves the privacy of $\mathscr{M}_1$ iff there exists a homomorphism from J_2 into J_1 that preserves the critical constant $*$. This will be referred to as conjecture (*C*).

(⇒) If $\mathscr{M}_2$ preserves the privacy of $\mathscr{M}_1$, then for every query p, if $\vec{*} \notin p(J_1)$, then $\vec{*} \notin p(J_2)$. By combining this fact with Lemma 2, it follows that there exists a homomorphism from J_2 into J_1 preserving $*$.

(⇐) The proof proceeds by contradiction. Assume that there exists a homomorphism h from J_2 into J_1 preserving $*$, but $\mathscr{M}_2$ does not preserve the privacy of $\mathscr{M}_1$. We will refer to this assumption as assumption (A_1). From assumption (A_1) and the discussion above it follows that there exists a query p over S such that $\vec{*} \notin p(J_1)$ and $\vec{*} \in p(J_2)$. Let h_2 be the homomorphism from p into J_2 mapping its free variables into $*$. Since the composition of two homomorphisms is a homomorphism, this means that $h \circ h_2$ is a homomorphism from p into J_1 mapping its free variables into $*$, i.e., $\vec{*} \in p(J_1)$. This contradicts our original assumption and hence concludes the proof of conjecture (*C*).

Conjecture (*C*) witnesses the decidability of the instance-independent privacy preservation problem: in order to verify whether $\mathscr{M}_2$ preserves the privacy of $\mathscr{M}_1$ we only need to check if there exists a homomorphism of $I_{\mathsf{S}}(\Sigma_2)$ into $I_{\mathsf{S}}(\Sigma_1)$ preserving $*$. □